(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/26061 A1

(51) International Patent Classification[7]: G07F 7/08, 7/10

(21) International Application Number: PCT/SE00/01842

(22) International Filing Date:
22 September 2000 (22.09.2000)

(25) Filing Language: Swedish

(26) Publication Language: English

(30) Priority Data:
9903575-0 1 October 1999 (01.10.1999) SE

(71) Applicant *(for all designated States except US)*: **AB TRYGGIT** [SE/SE]; Torred 4164, S-429 34 Kullavik (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **BRYNIELSSON, Thore** [SE/SE]; Torred 4164, S-429 34 Kullavik (SE).

(74) Agent: **AWAPATENT AB**; Box 11394, S-404 28 Göteborg (SE).

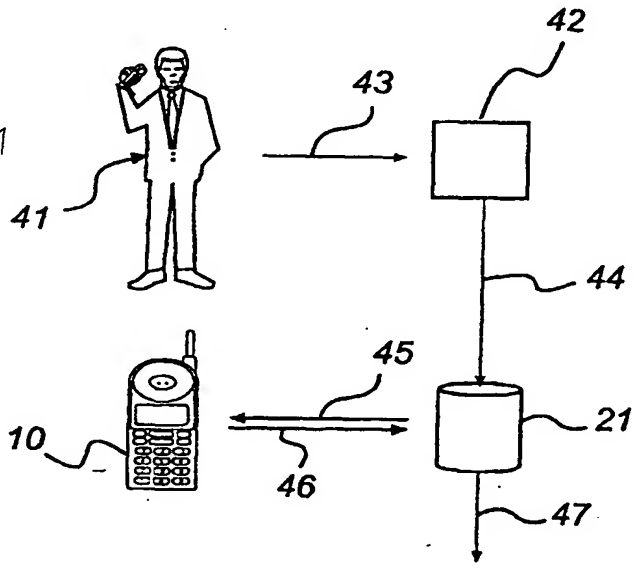
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KR (utility model), KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR AUTHENTICATION OF A SERVICE REQUEST



(57) Abstract: The invention concerns a method and a system for authentication of a commission from a customer (41) to a service provider (42), according to which a set of randomly generated code words has been stored in a memory circuit associated with a mobile-telephone subscription in a mobile telephone (10) as well as in a database (21) together with an association to said mobile-telephone subscription. The method comprises the steps of determining the identity (43) of the customer, of identifying the mobile-telephone subscription on the basis of the identity of the customer, of retrieving a code word (46) from the memory circuit, and of checking the presence of said code word in the code word set in the database (21) that is associated with said mobile-telephone subscription, in order to thus authenticate the commission.

WO 01/26061 A1

6/prts

METHOD AND SYSTEM FOR AUTHENTICATION OF A SERVICE REQUEST

Technical Field

The present invention concerns a method and a system for authentication of a request from a customer to a service provider.

Technical Background

A constantly recurring problem on the market in the case of purchases for which credit cards or bankcards are used is to establish the identity of the card user. Usually, each card has a specific code, for instance a four-digit number code, which in some stores may be inputted in a terminal in conjunction with the purchase. However, this is not a particularly attractive solution for an individual possessing a dozen cards, each having its specific code. Restaurants, for example, often employ the method of requesting the customer to sign a slip in confirmation of the transaction, and the signature serves as a post-check, should any doubt arise about the payment. This means that only long after the event will the cardholder notice if an unauthorized individual has utilized his card without his knowing. It might even happen that the personnel of the restaurant fraudulently charge the card with several transactions during the period when they alone have access to the card. It is often sufficient that a dishonest person gets hold of the number of the card to enable him to use the card on a later occasion.

According to prior-art technology intended for situations wherein a customer has recurrent contacts with

e.g. a bank, the customer is equipped with a list of codes hidden by a rub-off film. The bank has access to the same list, which may be stored e.g. in the bank computer system. Each time the customer requests a transaction, for instance by telephone, he exposes one of the code number by rubbing off the film and then discloses the exposed number to the bank. The number is compared against the list in the bank, and a match ensures that the customer is the person he claims to be, or at least is in possession of the rub-off list in question.

According to prior-art systems devised to provide secure transactions for instance on the Internet, the user must have access to a small electronic device at the time of the transaction. Codes are exchanged between the computer and the electronic device in order to ensure that the user actually has access to the electronic device. This technology is employed above all in conjunction with banking services on the Internet when a customer uses the service comparatively often.

The solution involving the individual-related electronic device does, however produce two problems:

In the first place, it is possible for a skilful expert to copy the electronics, for example the ROM memory, of an electronic device to which he has access albeit briefly. The electronic device may then be returned to the owner who suspects no mischief. From then on, there is no possibility for the computer system to ascertain whether a request is made by the owner or the dishonest person.

In the second place, an electronic device is specific to each service provider, which means that a user of several services must carry with him several

electronic devices. Consequently, there is a risk that he has forgotten the electronic device that is required for the occasion. In addition, it reduces the user's chances to keep an eye on all electronic devices, and a dishonest person can easily use a stolen device or copy a "borrowed" device before the user has had time to miss it.

When credit cards are used for payment over the Internet, generally only the number of the credit card serves as the authenticity check. It is possible to encrypt the credit card number, but if the encrypting code is cracked, a dishonest person could use the card comparatively freely until the time when the user receives a bill, usually at the end of a month. Electronic devices of the kind described above could of course be used to increase security, but the problems related to copying of the electronics of the device and the need for several devices do, of course remain.

Some providers of services offer systems on the Internet, according to which a person must first register as a customer and only then is he allowed to make purchases using his credit card. Like the system involving the electronic devices, these systems suffer from the disadvantage that they are specific to each service provider, making the user's life very complicated as he has to have contact with several service providers.

Other common services for which authentication of a user's authorization is needed are for logging in into computer systems and admittance into security-classified premises. These systems are based almost exclusively on the presentation of a user ID in conjunction with a code or a password, which in some systems are changed according to predetermined routines, or on security pass

cards and an associated code. Generally speaking, the fact is that in our society a multitude of codes exists which it is difficult for the individual to remember. He might therefore be tempted to write down the codes somewhere, which reduces security.

The combination of disclosure of a code and an electronic device, which has to be physically available, improves security but at the cost of requiring several devices. Consequently, this technology hardly presents a universal solution to the problems outlined above.

There is therefore a need for a uniform system that might be used with several types of service requests and that allows the authenticity of the customer or user to be verified in a simple manner.

Definitions

In the following description, a number of expressions will occur, which are defined as follows.

By the expression "commission" is to be understood generally a service that a person wishes to be rendered by a provider. For example, a commission could be a financial transaction delivered by a bank or similar establishment, but a commission could equally well be a request for admission into a building or for log-in into a computer system. To order such a commission is referred to as a "service request".

By the expression "service provider" is to be understood both the company carrying out the commission (such as a bank, a credit card company or a security company) and the equipment used to implement the commission (such as a door lock, an automatic teller machine or a computer system in log-in situations).

The "customer" is the individual requesting the commission from the service provider, and in the following description, the customer and the service provider are also users of the method and the system in accordance with the invention.

By the expression "database" is to be understood the data-storage memory unit as well as the software processing volumes of data and executing operations for instance for the purpose of comparing volumes of data.

By "mobile telephone" is to be understood herein a portable telephone, such as a cellular telephone (e.g. GSM) or the like. The expression naturally includes any portable telephones that may be developed in the future.

Purpose of the Invention

A first purpose of the present invention is to solve the problems outlined above and to make it possible to satisfactorily authenticate a customer requesting a service.

A second purpose of the invention is to make it possible to authenticate a customer requesting a service, by means of a universal method that may be made use of by several service providers without the provider requiring specific equipment.

Summary of the Invention

These purposes are obtained in accordance with the teachings of the invention by means of a method and a system defined in the independent claims 1, 13, and 14.

Thus, in accordance with the invention two identical code word sets are provided for each customer, one set being stored in a memory circuit in a mobile telephone and the other one being stored in a database.

Authentication is performed by identification of the mobile-telephone subscription, extraction of a code word from the memory circuit, and the code word is checked against that code word set in the database that is directly or indirectly associated with the mobile-telephone subscription. The relative order of the above operational steps could, of course, be different; for example, the code word could be extracted from the memory circuit prior to identification of the mobile-telephone subscription.

One advantage of the method and system according to the invention compared with prior-art technology is that the code words are of a use-once-only character combined with the fact that no predictable algorithm is used to derive the next code word. To gain knowledge of the code words in a set requires that the memory circuit of the mobile telephone be actually physically stolen or else copied electronically.

In addition, the method and the system according to the invention may be used by an unlimited number of service providers. The only condition required of the service provider is possession of equipment by means of which he is able to establish connection with the database and transfer the code word and the identity, and to receive the results of the authentication. In addition, this means that by blocking his mobile-telephone subscription in the database, the user may easily block all services that make use of the system. One alternative is that the service provider himself owns the database or a subset thereof.

An additional advantage is that the system may be used completely in parallel with and independently of existing security systems. Thus, each service provider

may choose on his own whether he wishes to join the system and thereby improve the security of his existing system.

Preferably, the code word is retrieved from the memory circuit in a predetermined order, which improves the security of the authentication further. Not only is a check made to establish whether or not the code word is included in the code word set that is associated with the stated identity, but also a check is made as to whether the code word is the correct one within the set.

In the memory circuit, it is possible to indicate when a code word has been used, and a similar indication may be made in the database. This possibility ensures that the memory circuit and the database agree as to from where in the predetermined sequence that the next code word is to be extracted. Consequently, the memory circuit and the database are prevented from getting "out of phase". This system may be equalled to the situation, wherein the customer carries on him a list of code words that are hidden by a rub-off coating. To use a code word, the customer needs to expose it by rubbing off the coated and the service provider exposes the corresponding hidden code word from his list in the same manner and compares the two. In order for the customer to be accepted, the correct list must be used, and in addition, the correct code word on the list.

One consequence of this procedure is that a dishonest individual, who has secretly gained access to a person's code word set, for example by having copied the memory circuit by electronic means, will only be able to use the memory circuit, if the person has not already made a request and in conjunction therewith used the next code word. Should the dishonest individual actually

succeed in accomplishing a request, the fraudulent action will be revealed when next the person is to make a request, since the code word he then indicates will not be accepted. The mobile subscription will then be blocked, and the damage is minimised. This should be compared with the situation according to prior-art technology, when a security device, copied secretly, may be used by a dishonest individual until the owner receives an irregular account statement or similar information.

The step of identifying the mobile-telephone subscription preferably includes the steps of determining the identity of the customer, and based on the identity of the customer, identifying the mobile-telephone subscription. The identity of the customer may consist of suitable data, such as the personal identification number, a credit card number or a mobile-telephone number. The concept "identity" in this case actually only indicates the existence of a direct connection to an individual, and the data representing the identity might be exchangeable. For instance, the identity data from the customer to the service provider could be supplied in the form of e.g. the number of a bank card or a security pass card together with the associated code, or a user ID together with an associated code, and from the service provider to the database in the form of a mobile-telephone number or a predetermined ID number. However, the database must be able to associate the received identity data with a predetermined code word set, normally via the mobile-telephone number, in order thus to be able to check that the given code word has been retrieved from the correct memory circuit.

In accordance with a preferred embodiment, a request is sent to the customer to state a code word. The customer thus can request a service in a conventional manner, whereupon the service provider, as an additional security measure, demands a code word, which the customer retrieves from the mobile telephone. Preferably, the service provider in this case is in possession of information regarding which ones of its customers are connected to the system in accordance with the invention, and as the case may be, sends an inquiry to the database. The database thereafter requests that the customer state a code word.

The request may be forwarded to the mobile telephone via the telecommunication network, and the code word may be transferred from the mobile telephone to the database via the telecommunication network. Preferably, the customer gives his acceptance of transmission of the code word by pressing suitable keys on the mobile-telephone keypad. Because in this manner two separate communication routes are made use of, on the one hand a route between the service provider and the database and on the other between the database and the mobile telephone, security is improved additionally. A dishonest individual, who has caught and distorted information along the first communication route, has no possibility of predicting which mobile-telephone subscription or base station will be used as the next step of the authentication process.

A request forwarded to the mobile telephone, for example in the form of an SMS message or the like, may contain information on the transaction. This may be advantageous, for example in a situation when the card has been swiped through the card reader and has been accepted by the card company, but when the transaction

amount has not yet been established. When the entire authentication process has been concluded, a dishonest individual could then state an erroneous amount, thus charging the account of the customer with too high an amount. By means of an SMS message as indicated above the fraud would be detected by the customer, who thus is informed of the fraudulent request to his mobile telephone and then is able to deny acceptance of the transaction.

The fact that the mobile telephone is contacted directly gives the user a possibility of detecting a fraudulent action as it is being perpetrated. He can then block the mobile-telephone subscription immediately, or block the card or the service exposed to the fraud. Let us assume that someone has stolen or copied a person's credit card and in addition has succeeded in obtaining the next code in that person's memory circuit. When the card is being used and a transaction is accepted by the database, a message is sent to the person's mobile telephone, whereupon the person is apprised of the fact that someone has used one of the code words in the memory circuit. Another possibility is to delay the request for a code word to the customer for a predetermined length of time, or to make use of two confirmations, spaced apart in time. This procedure would prevent a dishonest individual from using a mobile telephone, which is later returned to the owner, without the owner being aware thereof. The length of the delay may be adapted to ensure that the owner of the mobile telephone will have time to miss it and block it before a code-word request is sent to the mobile telephone and the order thus confirmed.

At the same time, this method permits a customer to allow a third person to use the customer's card for a

particular service, for example to buy some merchandise. Irrespective of his whereabouts, the customer is informed of the purchase on his mobile telephone, and makes the final confirmation via his mobile telephone.

Particularly in the case of service requests via the Internet, it is advantageous that a request from the database or the provider of the service is made directly to the mobile telephone, since all Internet-transferred information is accessible to others to a larger or smaller extent. An SMS message made to the customer's telephone therefore is an excellent acknowledgement of the correctness of the transaction.

In accordance with another embodiment of the invention the identity of the customer and the code word retrieved from the memory circuit are transferred to the service provider, the mobile-telephone subscription associated with the customer is identified by the service provider, and the identities of the code word and the mobile-telephone subscription are transferred to the database by the service provider. This method allows the customer to transfer, directly in conjunction with the request, his identity as well as a code word to the service provider. The identification of the mobile-telephone subscription is then effected either by the service provider or by the database.

In accordance with a further embodiment of the invention a second code word is retrieved from the memory circuit and transferred to the database in order to additionally verify the authenticity of the request. The code words of the set may be associated with one another in groups comprising different numbers of code words, to be used for different types of service requests of different security levels.

The first code word may be transferred from the customer to the database, perhaps via the service provider, whereupon the database issues a request to the customer to state a second code word, and finally, the second code word is transferred from the customer to the database. The request to the customer may be effected in the same way as in the case of the request described above. One possibility thus is that the customer receives two successive requests to the mobile telephone to transfer a code word. Another possibility is that the customer first states a code word directly in conjunction with making his request and thereafter is asked to state an additional code word. Obviously, several other possibilities exist, and in particular the PIN code of the mobile telephone may be made use of as one means of increasing authentication security.

According to one embodiment of the invention, also position data associated with the mobile-telephone subscription are stored in the database. In the authentication process, the memory circuit is located, and the position data received may be compared with the position data stored in the database. This method may be used to geographically restrict the area within which the customer can effect certain types of service requests. For example, purchases above a certain amount may be limited to a few, predetermined locations, which increases security further. This geographic check can also be applied for logging-in into a computer system, which perhaps is allowed only from the work premises or from home. Alternatively, position data in the database could be an IP address, allowing log-in processes or Internet transactions to be restricted to a specific

computer unit, without such information being available to the service provider or anywhere on the Internet.

Brief Description of the Drawings

The present invention will be described in more detail in the following with reference to the accompanying drawings, which for exemplifying purposes show preferred embodiments of the invention. In the drawings:

Figs 1a-b show two code word sets in accordance with the invention,

Fig 2 shows a mobile telephone in accordance with the invention,

Fig 3 shows a database in accordance with the invention,

Fig 4 shows the manner of retrieval and storage of the code-word sets of Fig 1,

Figs 5a-e show five different preferred embodiments of the method according to the invention, and

Fig 6 illustrates the method in accordance with the invention in a more detailed view.

Description of Preferred Embodiments

Figs 1a-b show two examples of a code word set 1 consisting of a plurality of codes 2 in the form of four-digit or six-digit number combinations. These number combinations are extracted at random and have no deducible relationship, neither as to their composition nor as to their sequence. The codes may be arranged in groups 3 containing two or several codes 2 in each group.

Since each code in itself is entirely independent of the others, there is nothing to prevent one combination

of numbers to appear several times in the same set, or even within the same group.

The code-word set 1 is associated with an identity 4, which is directly or indirectly connected with a mobile-telephone subscription. In the shown example, the identity consists of a mobile-telephone number 5.

The mobile telephone 10, shown schematically in Fig 2, is equipped in the conventional manner with a keypad 11, a display 12, and a receiver/transmitter 13. The mobile telephone also has a memory circuit 15, for example a SIM card or similar smart card, which contains data 16 pertaining to the mobile-telephone subscription. For example, a SIM card may comprise information on the telephone number of the subscription and on how much credit remains in the customer's account with the mobile service provider. In accordance with the invention, the memory circuit 15 is also provided with a code word set 17 that is associated with the subscription.

The SIM card may be provided with a subscription ID and a code word set before being delivered to a retailer under conditions of extreme security, for example in the form of a seal of some kind. The customer, who buys or in some other way gets hold of the SIM card checks that the seal has not been violated and thereafter arranges the SIM card in his mobile telephone, which allows him to use the telephone.

In addition, the mobile telephone shown in Fig 2 comprises means, such as software 18, devised to retrieve from the memory circuit 15 a code word from the code word set 17, and to transmit the code word by means of mobile-telephone communication, for example in a SIM message. Software having this function may be developed by the expert in the field. The software 18 may also transmit a

code word via a communication port or an IR port. In addition, a retrieved code word may be shown on the display 12.

Furthermore, the software 18 is arranged to receive a code word and to compare the code word with the code word set in the memory circuit. The code word may be inputted by means of the keypad 11, or else be received by means of mobile-telephone communication directly to the receiver 13 of the mobile telephone, for example through reception by the mobile telephone of a SMS message.

Preferably, the mobile telephone is arranged to be set in a dormant state, wherein it does not receive any telephone calls but wherein it is capable of receiving and transmitting SMS messages. This function may be devised by an expert in the field.

In the database 21 shown in Fig 3, a plurality of code-word sets 22 are stored, each one having an identity 23 that is associated with a mobile-telephone subscription, the corresponding SIM card of which comprises an identical code word set.

In addition, each set 22 can be associated to one or several position indications 24. The position indications could for instance be locations where the customer has indicated that he wishes to be able to make a certain type of requests.

The database 21 is furthermore provided with communication means 25 able to receive a question and to provide the results of the authentication process. For example, the communication means 25 could be a modem arranged to communicate with the service provider, for example to receive a code word and an identity from the service provider, and to transmit confirmation to the

service provider that the authenticity of the commission is verified. The communication means 25 could also be arranged to communicate with the mobile telephone via the mobile-telephone network, for example by way of SMS messages.

The database 21 is also provided with means, preferable software 26, arranged to perform searches in the database and to verify e.g. that a specific code word exists in the code word set 22 in the database associated with a predetermined identity 23.

Fig 4 illustrates how code-word sets 1 are formed and stored.

In a completely independent computer system, combinations of numbers are created at random in accordance with algorithms that cannot be predicted from the outside (Step 31). This procedure ensures that nobody can predict which code words are included in a particular code word set, and can easily be devised by an expert in the field. The combinations of numbers are arranged in groups and sets (Step 32), in accordance with algorithms, which in themselves may be allowed to be known outside the computer system. In addition, the computer system is provided with a series of mobile-telephone numbers which are supplied by a mobile-telephone service provider, and which associate each code word set with a particular telephone number (Step 33).

The sets are then distributed (Step 34) to companies that equip the SIM cards with data, where each code word set is stored on a SIM card (Step 35), the latter either prior to or after the storage having been attributed to the mobile-telephone number associated with the mobile-telephone number.

In addition, the sets are also distributed (Step 34) to the database, where they are also stored (Step 35). The sets may be stored on access-protected data carriers, such as coded and sealed CDs, which are distributed in a safe manner, for example by means of couriers. If the computer system forming the sets is connected to the database, this part of the distribution may be effected safely electronically.

Figs 5a-e illustrate generally five different varieties of the manner in accordance with the invention of implementing the process of authenticating a request from a customer 41 to a service provider 42. In all cases, the customer 41 has access to a mobile telephone 10 in accordance with Fig 2.

In accordance with the method of Fig 5a, the customer initially states his identity 43 to the service provider 42. Normally, he does this in conjunction with making his request, in which case he provides e.g.a user's ID, a credit card number, or other information allowing the service provider to identify the customer.

The service provider possesses information on which customers are connected to the system in accordance with the invention, and is able to associate a mobile-telephone subscription with the identity of the customer. The service provider 42 sends a query to the database 21, and transmits to the database 21 the identity of 23 of the mobile-telephone subscription, usually in the form of a mobile-telephone number but possibly in the form of another identification associated with the mobile-telephone subscription. It should be understood that ead the identity 43 of the customer could be tted to the database 21 and the mobile-telephone n in question be identified by the database.

The database thereafter sends a request 45 to the mobile telephone 10 via the telecommunication network, for example an SMS message, or the like. The message 45 contains particulars of the request, which are shown on the display 12, thus allowing the customer to check the correctness of the request. In the affirmative, the customer may confirm the fact in any suitable manner, for example by pressing a particular key on the keypad 11 twice. For example, the customer may receive a message on his mobile telephone of the type reading "Credit card purchase $35 at BurgerKing. Press OK to confirm", or "You are now logging-in into your workplace, Press OK to confirm". The customer then presses the OK key. An additional confirmation step of the type "Are you sure Y/N" might be advisable as an extra check. The software 18 of the mobile telephone then retrieves from the SIM card 15 the next, not yet used code 46 and transmits the latter from the mobile telephone 10 to the database 21. Simultaneously, the transmitted code word is marked as used on the SIM card. The request 45 from the database could also contain a code word (not shown), which is checked by the mobile-telephone software 18 against the code word set 17 in the SIM card 15.

Another possibility is that the database 21 contacts the service provider 42, who in turn asks the customer for a code word, which the provider returns to the database 21.

As the database 21 receives the code word 46, the latter may be compared with the code word set 22 that is associated with the mobile-telephone subscription. Should the check fail, for example because the code cannot be found in the code word set in the database that is associated with the mobile-telephone number, information

of this fact is transmitted to the service provider, who may refuse to perform the service, for example by refusing access to a computer system or stopping a transaction. On the other hand, if the check is positive, i.e. the stated code is the correct one, a go-ahead signal 47 is transmitted to the service provider 42, who may then perform the service. At the same time, the code word received is marked as being used up.

In accordance with the method shown in Fig 5b, the customer 41 states a code word 4 in conjunction with giving his identity 43 as described above. For example, the customer 41 may read a code word 46 from the display 12 of the mobile telephone 10 and transmit that word to the service provider 42. Alternatively, a data transmission port 19 in the mobile telephone may be used to transmit a code word to the service provider.

The service provider then issues a query 44 to the database 21 and in addition to transmitting the identity as described above, he also transmits the code word 46. The database 21 checks the code word as described above and sends a go-ahead signal 47 to the service provider 42.

The method shown in Fig 5c actually is a combination of the two previous methods. The customer 41 first states a code word 46' as he makes his request in accordance with Fig 5c and then receives a request 45 for an additional code word 46'' in accordance with Fig 5a.

In order to further increase security, the software 18 may be arranged, in the case of certain requests, such as purchases above a predetermined amount, to demand the user's PIN code as a condition for retrieval and transmission of the code word. This arrangement means that a dishonest individual who has got hold of a mobile

telephone that is in the switched-on state still has to know the owner's PIN code.

In addition, the position data stored in the database could be used to increase security. The base station over which the mobile telephone communicates can be identified comparatively easily, and a comparison with the stored position data may be performed. Likewise, it may be possible to equip the mobile telephone with a GPS navigator or similar means, allowing the mobile telephone to make his position known with great accuracy. The position check could in this case be effected in two steps, the first one roughly with respect to the base station and the second one more precisely, with respect to longitude and latitude.

The method shown in Fig 5d could be regarded as a variety of the method shown in Fig 5b. In this case, the database 21' is owned by the service provider 42, for which reason no external communication is required from the service provider 42. The database 21' could be a subset of a larger database 21. This method could be used for instance when a person is to be given access to a protected object, such as a car. The car is equipped with a database 21' comprising a number of code words, and the user may be simply identified by means of his mobile telephone.

The method shown in Fig 5e is very similar to the method of Fig 5b, but the check vis-à-vis the database 21 is effected only after some delay 48. If the mobile telephone subscription does not satisfactorily manage the credit check and ID check, the mobile telephone is blocked in the service-provider system. Examples of use of this method are payment of public-transport fees and parking fees.

Further varieties and combinations of these methods are possible within the scope of the invention. The number of code words exchanged between the mobile telephone and the database may vary, depending on the desired security level.

In the following, some examples will be given of situations, wherein an authentication method in accordance with the invention is particularly suitable.

Restaurants

A guest who has dined in a restaurant requests from his credit card company or the like the service of paying the restaurant bill, using funds available in the guest's own account or in the account of the account card company (credit card). The card company thus is the service provider and the guest the customer.

In the conventional manner, the credit card is handled by the restaurant personnel, who check the card for verification of its number, its validity, whether funds are available in the account, that the card is not blocked, etc. In this manner, the card company receives information on the identity of the customer, for example through the unique card number. In accordance with a commonly used technology, the card is swiped in a card reader, which via a modem contacts the card company and checks the transaction.

In a register, the card company has stored data showing that the customer is connected to the system in accordance with the invention, and identifies the telephone number of the mobile-telephone subscription. It is transmitted to the database, which thereafter contacts the mobile telephone via the telecommunication network and receives a code word (Fig 5a).

Alternatively, the customer uses his mobile telephone in order to state a code word as he makes his request (Fig 5b). The code word may be disclosed to the restaurant personnel, who contacts the card company via the card terminal and transmits the code, or else it may be transmitted from the mobile telephone to the card terminal by means of some kind of communication means, such as an IR port.

When the authenticity of the code word has been verified by the card company, a go-ahead signal 47 is sent to the restaurant, and a receipt is printed.

Internet Transactions

The method is similar when a computer user wishes to make a transaction on the Internet or the like, for example transfer funds from one of his bank accounts, or make purchases using a credit card. In this case, the computer user is the customer requesting a service in the form of a transaction. The service provider could be a card company as above, or the customer's own bank.

In this case, the identity of the customer is transmitted by input of for example a personal identification number and the associated password, or a credit card number or the like. Inputting may be effected in a screen display on a WWW page, and the contents of the page be sent to the owner of the page through pressing a key.

If a method in accordance with Fig 5a is used, the process is identical with that of the example described above, and within minutes the customer receives an SMS message on his mobile telephone and is able to confirm the request by pressing suitable keys. If a method in accordance with Fig 5b is used, according to which the customer reads a code word from the display of the mobile

telephone, the code word may be transmitted in the same manner as the identity, either on the same WWW page or on a following page appearing immediately after acceptance of the identity.

Log-in/Passing-in

Another category of services that is suitable for authentication checks in accordance with the invention is requests for log-in into a computer system. In this case, the customer is the person requesting to access the system, the service is admittance of the person into the computer system or the like, and the service provider is the company or computer system responsible for security.

The customer states his identity when logging in according to prior-art technology, and in conjunction therewith he enters for example a user ID including a password. The service provider can then contact the database, which demands a code word directly from the mobile telephone in accordance with Fig 5a. Alternatively, the customer may be given a possibility in accordance with Fig 5b to indicate, via the keypad, a code that has been read on the mobile-telephone display.

The procedure of allowing physical passing into premises or an area is similar to that of log-ins. For example, the identity of the customer could in this case be provided by swiping a security-pass card through a card reader or inputting a code on a door lock.

Example of a Detailed Chain of Events for Credit card Payments

With reference to Fig 6, a more detailed description will be given below of a possible chain of events necessary to allow a legitimate customer to implement a request with a high degree of security. If the security of the request is not classified to be of the same high

degree, certain operational steps could be excluded from the chain of events. Preferably, it is the computer of the service provider that determines the security classification of the request and whether or not a tip should be given at the point of sale. In this manner, the rest of the chain of events is controlled based on the security classification and on whether or not a tip should be given.

a) The customer 41 hands over a credit card 51.

b) The credit card is swiped through the card reader terminal 52 and the amount to be paid (inclusive of wardrobe fees and the like, if any) is inputted into the terminal. The terminal 52 generates a message of the desired payment, comprising e.g. the credit card number, the number of the card terminal and the amount to be paid.

c) The card terminal sends the message generated in (b) to the computer of the credit card company (service provider 42).

d) The computer of the credit card company checks the transaction for sufficient credit, and if the check is positive, the computer generates a message concerning the transaction (seller and amount, and so on), stating the number of the request, the security classification of the request, whether a "tip" should be given, and the mobile-telephone number of the credit card holder.

e) The computer of the credit card company transmits the message received in (d) to the database 21.

f) The database 21 retrieves the next not-used code word, checks with the mobile operator 54 concerned whether the mobile telephone is on an accepted location, and generates a message, demanding confirmation of the request. The message comprises e.g. data as to the

seller, the number of the request, security classification, whether tips are expected, and the next non-used code word (576362).

g) The database 21 transmits the message that was generated in (f) to the customer's mobile telephone 10.

h) The mobile telephone checks the security classification concerned and whether a tip-payment situation exists. Based on the results of the check, the mobile telephone selects the routine to be followed. The mobile telephone presents the query on the display and asks for confirmation. The customer presses the OK key for confirmation. In cases of high-security classification, the mobile telephone requires that the customer inputs his PIN code or a corresponding pass word that only the customer knows. If a point of sale is involved (such as a restaurant) where tips are customary, a question will appear on the display of the customer's mobile telephone as to whether the amount should be increased, and the customer may then input a new, higher amount. The mobile telephone asks the customer to again confirm and if the customer does so, either one or two messages are generated, depending on the security classification. Both messages state e.g. the number of the mobile telephone, the number of the request, the seller, the amount, the final amount (in the case of a tip), the first non-used code word (576362) and the following non-used code word (805209) and, if the mobile telephone has an integrated GPS receiver, also the GPS co-ordinates are given. The mobile telephone registers the two code words as used up. The entire step (h) is processed by the software 18 of the mobile telephone 10, and this software may be developed by an expert in the field.

i) The mobile telephone 10 transmits the message generated in (h) to the database 21.

j) The mobile telephone 10 transmits the message generated in (h) to the computer 42 of the credit card company.

k) The database 21 checks the message received from the mobile telephone and if both code words are correct, an ID confirmation message is generated, which includes both code words, and the two code words are registered as being used up.

l) The data base 21 sends the ID confirmation message generated in (k) to the computer 42 of the credit card company.

m) The computer of the credit card company checks the message from the mobile telephone (j) and the ID confirmation message from the database (l) and executes suitable comparisons. If all data are accepted, a printing order is generated, which comprises suitable information, such as seller, buyer, amount, credit card number, number of request, date, time and verification number.

n) The printing order is transmitted to the card terminal 52.

o) The card terminal prints the transaction receipt 53.

p) The credit card 51 is returned to the customer, who signs the transaction receipt 53, keeping the copy while the seller keeps the original.

The following steps represent the customer's experience of the chain of events described above.

- The customer hands over his credit card in the usual way.

- On the display of his mobile telephone, the customer receives information on the payment, and he and confirms the commission by pressing two keys. When the commission is considerable (high security classification), the customer has to input his PIN code or other similar password between the first and the second confirmation, and if needed he adjusts the amount, i.e. he gives a tip.
- The customer signs the transaction receipt and keeps the copy, in the customary manner.

Additional steps: By pressing keys twice, the customer confirms the payment and also inputs, if required, the PIN code and increases the amount if a tip is to be given.

Steps that disappear: The customer need not show any identification papers.

The following sequence of steps represents the seller's experience of the above chain of events.

- The seller accepts the credit card and runs it through the reader of the card terminal, as usual.
- The seller inputs the amount via the card terminal as usual.
- The seller tears off the transaction receipt as usual.
- The seller makes sure that the customer signs the receipt of the transaction and keeps the original as usual.

Additional steps: None

Steps that disappear: The seller does not have to ask for identification papers, check the latter or register the number of the identification papers.

Possible Varieties of Locations Where Rapid Payment is Essential

In case of payment of smaller amounts in shops, kiosks, petrol stations, and the like, the confirmation might not necessarily have to be effected over the mobile network, since this procedure might take about a minute longer. Instead, the IR data transmission port 19 of the mobile telephone might be used. In this case, the card terminal is also equipped with a corresponding communication port (not shown) and software, as well as with a display, should the cash register not already have a display facing the customer. The communication port preferably is located on the display unit or close to the latter.

According to this embodiment, the seller swipes the customer's credit card through the reader, and inputs the amount, or receives it directly, for instance from the petrol pump that the customer has just used, i.e. in the manner in operation today. When this is done, the amount is shown on the display mentioned above, said display also requesting the customer to e.g. "Confirm payment by means of your mobile telephone". The customer then directs his mobile telephone towards the display and receives e.g. the name of the petrol station and the amount in question. By two confirmation key pressings on the mobile-telephone keypad, the first non-used code word is transferred to the card terminal and the display may show e.g. "Password received". From then on, everything functions as it does today.

It could be said that the mobile telephone replaces the control keypad commonly existing in many petrol stations, at least in Sweden. However, any person standing close by could make note of the code that is

being inputted, even if a screen is provided to make this more difficult. Should the person who just inputted his check code leave his card on the desk, this might constitute a temptation to a dishonest individual. Such a person could, for instance block the credit card from view by putting his hand over it and let it slide down into his pocket. The dishonest individual could then fill the family cars with petrol before the rightful owner notices that his credit card is missing, for instance when a week later he again intends to fill his car with petrol.

A consequence of the invention is that a code word is never used more than once, and in addition that normally nobody, neither the customer nor any one else, will ever set eyes on any code words whatsoever.

Conclusion

It should be understood that a number of varieties of the embodiments described above are possible within the scope of protection of the appended claims. For example, a large number of alternative authentication methods can be used with a system in accordance with the invention. In the same manner, equipment different from the one described herein could be used to implement the method in accordance with the invention.

CLAIMS

1. A method of authenticating a commission from a customer (41) to a service provider (42), comprising the steps of

forming a plurality of sets (1) of randomly generated code words (2),

storing one of said plurality of code word sets (1) in a memory circuit (15) of a mobile telephone (10), which circuit is associated with a mobile-telephone subscription,

storing an identical code word set (1) in a database (21) together with an association to said mobile-telephone subscription, and

at the time of requesting the commission, identifying said mobile-telephone subscription, retrieving at least one code word (46) from the memory circuit and checking the presence of said code word in the code word set (1) in the database that is associated with said mobile-telephone subscription, thereby authenticating the commission.

2. A method as claimed in claim 1, wherein the code word is retrieved from the memory circuit (15) in a predetermined sequence known to the database.

3. A method as claimed in claim 2, further comprising the step of registering, in at least in one of the memory circuit (15) and the database (21), when a code word (46) has been used, thus ensuring said predetermined sequence is followed.

4. A method as claimed in any one of the preceding claims, wherein the step of identifying the mobile-telephone subscription comprises the steps of

determining the identity of the customer, and,

based on the identity of the customer, identifying the mobile-telephone subscription.

5. A method as claimed in any one of the preceding claims, wherein a request (45) to provide a code word is sent to the customer.

6. A method as claimed in claim 5, wherein the request (45) is sent to the mobile telephone (10) via the telecommunication network.

7. A method as claimed in claim 5 or 6, wherein the code word is transmitted from the mobile telephone (10) to the database (21) via the telecommunication network.

8. A method as claimed in claims 1-3, wherein the identity (43) of the customer and the code word (46) retrieved from the memory circuit are transferred to the service provider (42),

the mobile-telephone subscription associated with the customer is identified by the service provider, and the code word (46) and the identity (23) of the mobile-telephone subscription are transferred to the database by the service provider.

9. A method as claimed in any one of the preceding claims, wherein a second code word (46'') is retrieved from the memory circuit (15) and is transferred to the database (21) to further authenticate the commission.

10. A method as claimed in claim 9, wherein the code words in the set are connected to one another in groups (3), said first (46') and said second (46'') code words being included in the same group of code words.

11. A method as claimed in claims 9-10, wherein said first code word (46') is transferred from the customer (41) to the database (21), the database sends a request (45) to the customer to provide said second code

word (46''), and said second code word is transferred from the customer to the database (21).

12. A method as claimed in any one of the preceding claims, further comprising the steps of

associating at least one position indication (24) with the mobile-telephone subscription and storing said indication (24) in the database (21), and,

each time a commission is requested, establishing the location of the memory circuit (15) and checking the position indication thus obtained against said position indication (24) stored in the database.

13. A method of authenticating a commission from a customer to a service provider, wherein a set (1) of randomly generated code words (2) has been stored in a memory circuit (15) associated with a mobile-telephone subscription in a mobile telephone (10) as well as in a database (21) together with an association (23) to said mobile-telephone subscription, comprising the steps of

establishing the identity (43) of the customer,

identifying the mobile-telephone subscription on the basis of the identity of the customer,

retrieving a code word (46) from the memory circuit, and

checking the presence of said code word in the code word set (22) in the database (21) that is associated with said mobile-telephone subscription, in order to thus authenticate the commission.

14. A system for authenticating a commission from a customer (41) to a service provider (42), comprising

a mobile telephone (10) having a memory circuit (15) associated with a mobile-telephone subscription,

means to enable the customer to disclose his identity (43) to the service provider,

characterized in that the system further comprises

a database (21),

a set (1) of randomly generated code words (2), said set stored in the first place in the memory circuit (15) and in the second place in the database (21), where it is associated with the mobile-telephone subscription,

means to identify the mobile-telephone subscription based on the identity (43) of the customer,

means to enable the customer (41) to retrieve a code word from the memory circuit (15) and to transfer said code word to the database (21), and

checking means (25, 26) for checking that said code word is present in the code word set (22) in the database that is associated with said mobile-telephone subscription, in order to thus authenticate the commission.

15. A system as claimed in claim 14, wherein said checking means comprises a communication means (25) for communication between the database (21) and the mobile telephone (10).

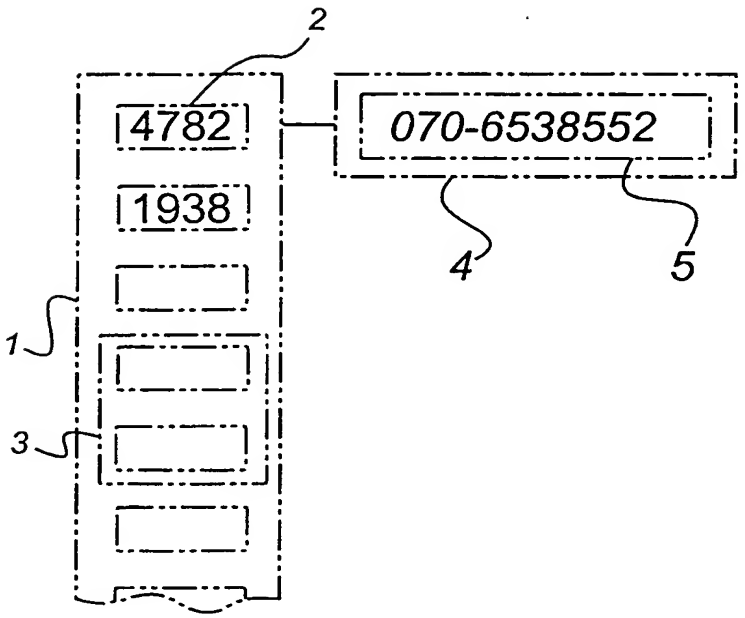


Fig 1

Code words in SIM and in database before start of current commission:

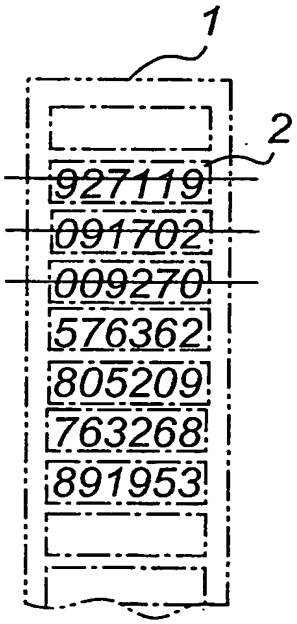


Fig 1b

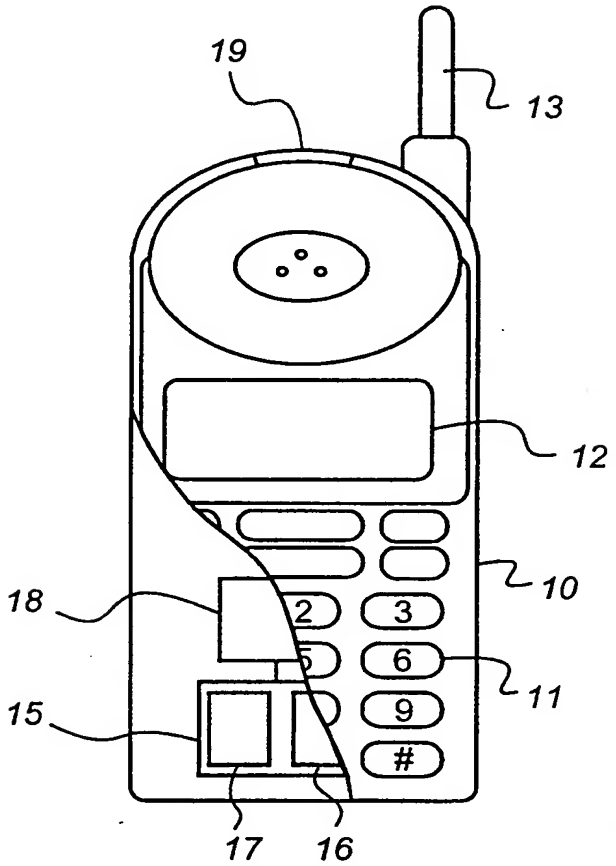


Fig 2

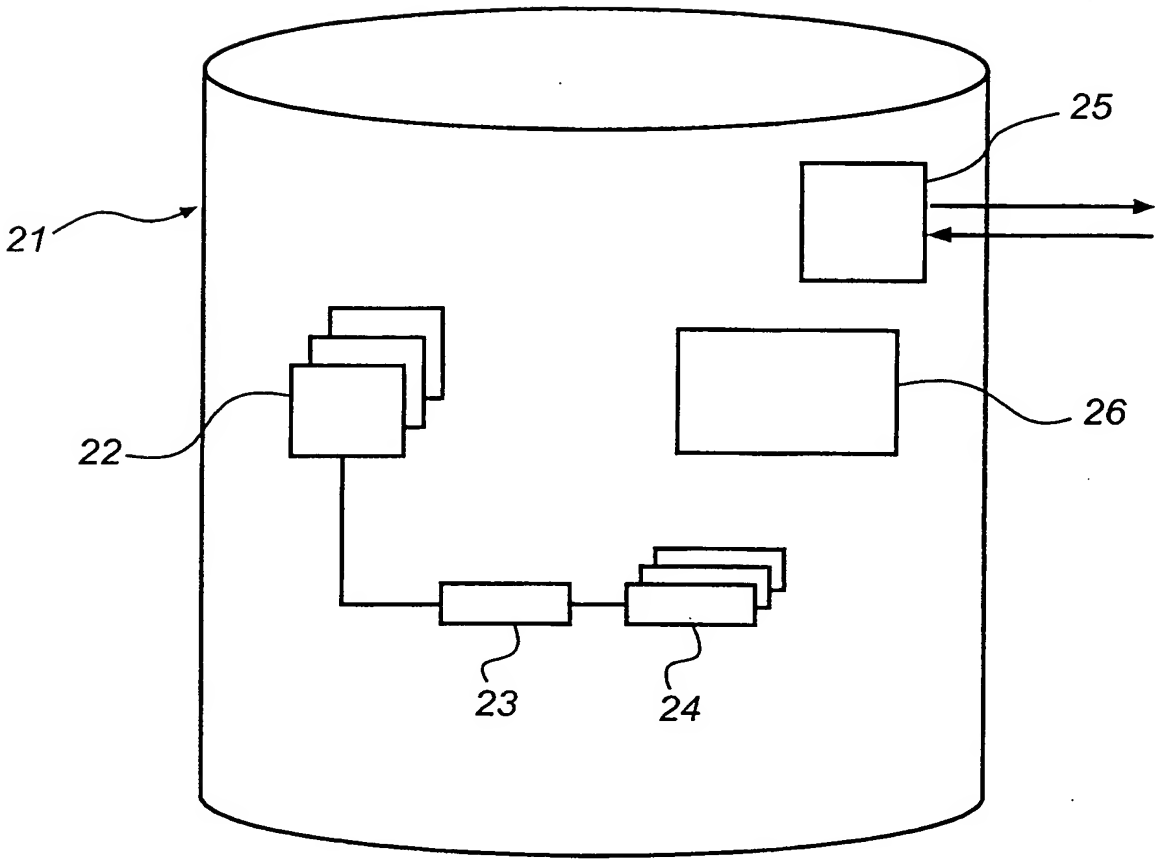


Fig 3

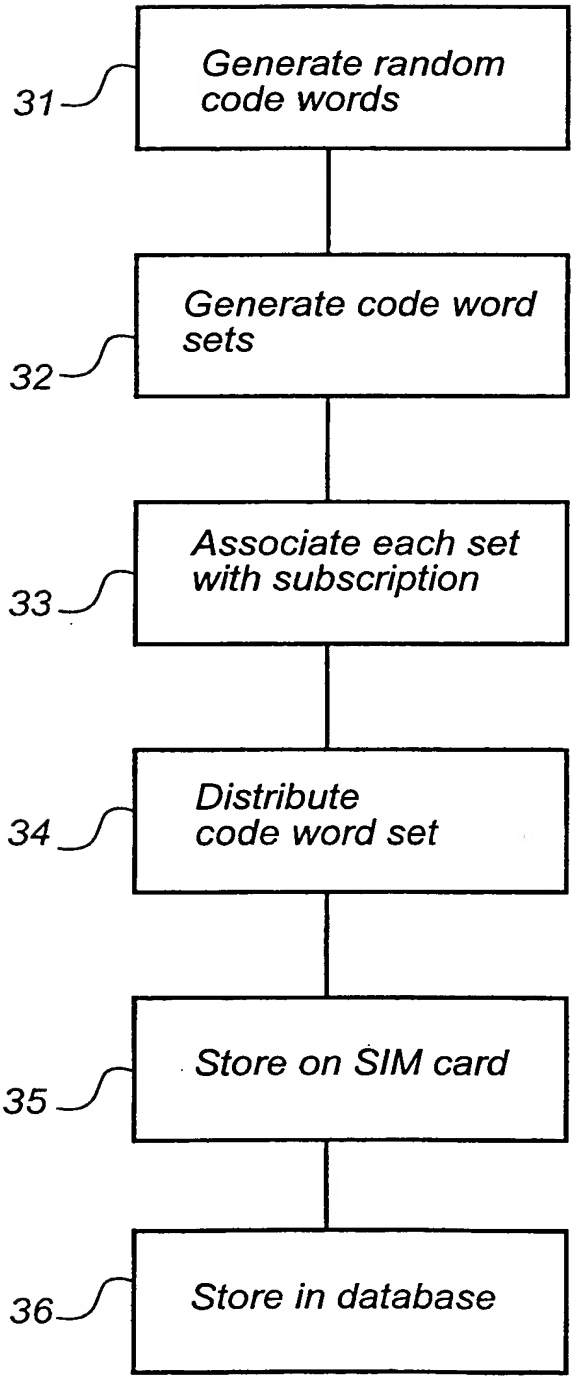

31
Generate random code words
32
Generate code word sets
33
Associate each set with subscription
34
Distribute code word set
35
Store on SIM card
36
Store in database

Fig 4

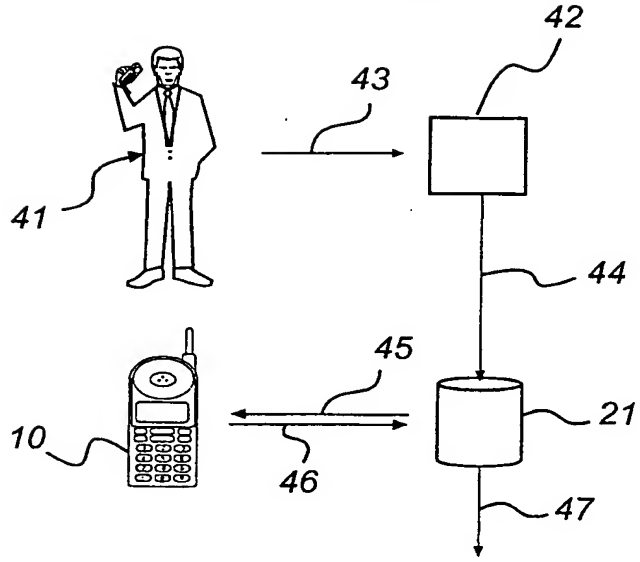


Fig 5a

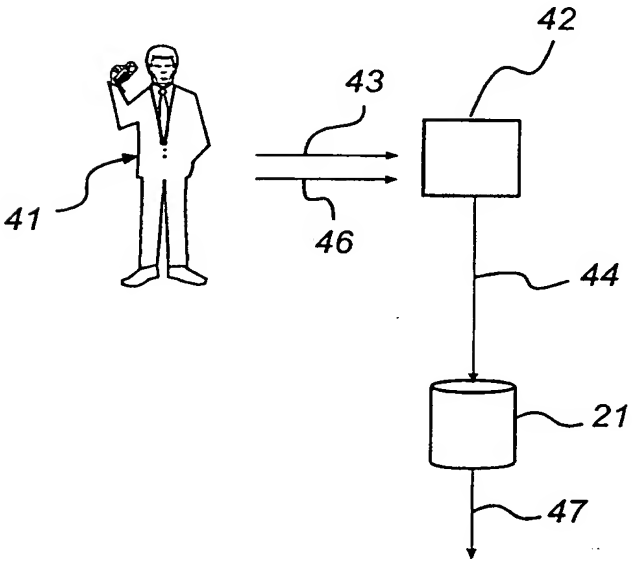


Fig 5b

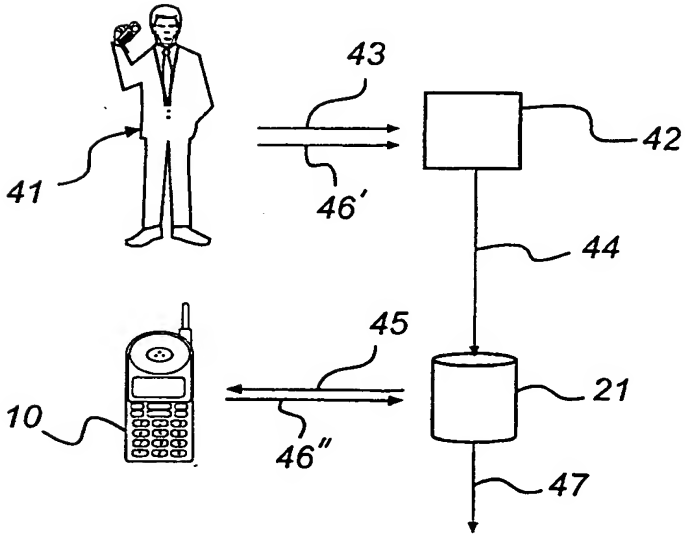


Fig 5c

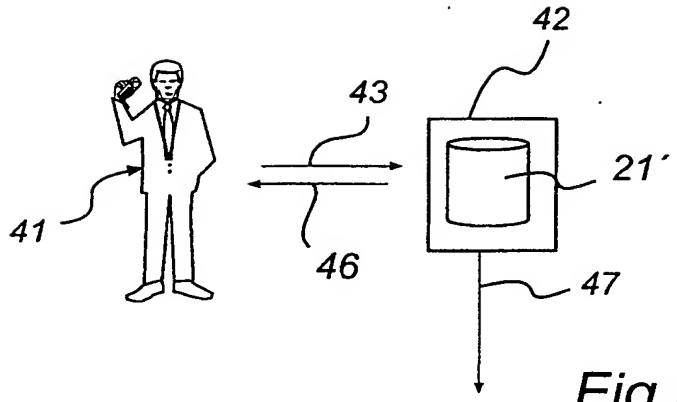


Fig 5d

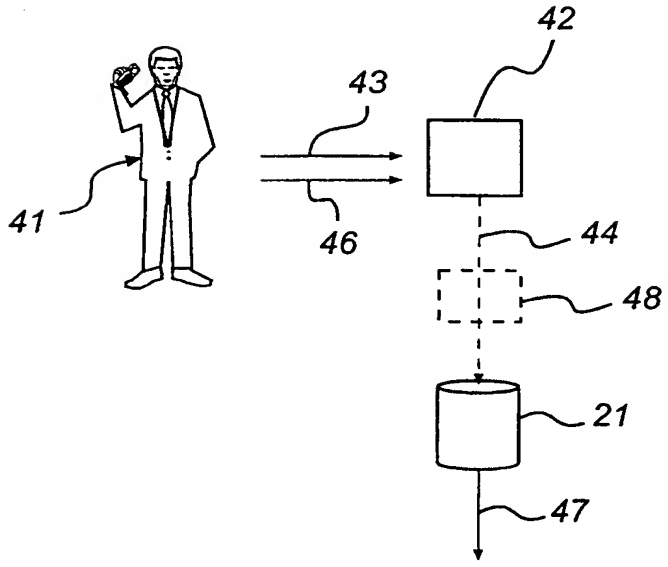


Fig 5e

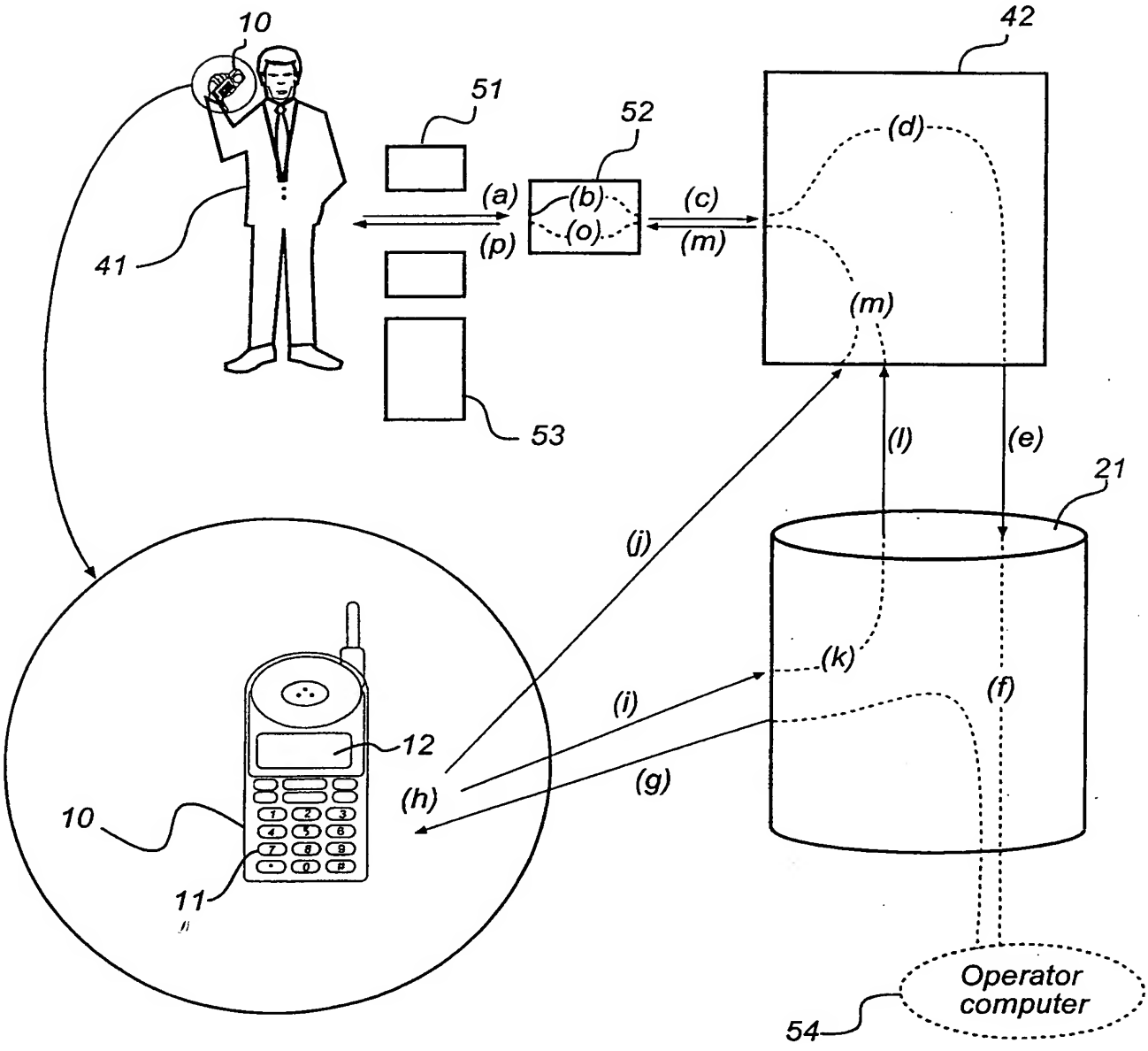

10
42
51
52
(d)
(a)
(b)
(c)
(o)
(p)
(m)
41
(m)
53
(l)
(e)
21
(j)
(k)
(f)
(i)
12
(h)
(g)
10
11
Operator computer
54

Fig 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01842

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G07F 7/08, G07F 7/10
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G07F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5878337 A (JOAO ET AL), 2 March 1999 (02.03.99), abstract ---	1-15
A	US 5708422 A (G.E.BLONDER ET AL), 13 January 1998 (13.01.98), abstract ---	1-15
A	WO 9945693 A1 (WALKER ASSET MANAGEMENT LTD.), 10 Sept 1999 (10.09.99), abstract ---	1-15
A	US 5416306 A (T.IMAHATA), 16 May 1995 (16.05.95), abstract --- --------	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2001	23 -01- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Gordana Ninkovic´ / itw Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/00

International application No.
PCT/SE 00/01842

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5878337 A	02/03/99	AU 3977597 A	25/02/98
		US 5903830 A	11/05/99
		US 6047270 A	04/04/00
		WO 9806214 A	12/02/98
US 5708422 A	13/01/98	CA 2176163 A,C	01/12/96
		EP 0745961 A	04/12/96
		JP 8339407 A	24/12/96
WO 9945693 A1	10/09/99	AU 2897299 A	20/09/99
		US 5999596 A	07/12/99
US 5416306 A	16/05/95	NONE	

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
PC-2006796		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/SE00/01842	22.09.2000	01.10.1999
International Patent Classification (IPC) or national classification and IPC7		
G07F 7/08, G07F 7/10		
Applicant		
AB TRYGGIT et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
05.04.2001	02.01.2002
Name and mailing address of the IPEA/SE	Authorized officer
Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. 08-667 72 88	Telex 17978 PATOREG-S Gordan Nincovic´ /OGU Telephone No. 08-782 25 00

Form PCT/IPEA/409 (cover sheet) (January 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/SE00/01842

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☐ the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the claims:
pages _____, as originally filed
pages _____, as amended (together with any statement) under article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the drawings:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language English which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☒ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheet/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2 (c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item I and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/SE00/01842

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-15	YES
	Claims		NO
Inventive step (IS)	Claims	1-15	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-15	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

Cited documents:

1. US 5878337 A (Joao et al), 2 March 1999
2. US 5708422 A (G.E.Blonder et al), 13 January 1998
3. WO 9945693 A1 (Walker Asset Management LTD), 10 Sept 1999
4. US 5416306 A (T.Imahata), 16 May 1995

The documents cited in the International Search Report represent background art.
The invention defined in claims 1 - 15 is not disclosed by any of these documents.

None of the cited documents gives any indication towards the claimed methods and a system for authenticating a commission from a customer to a service provider. No relevant combination of the cited documents would lead a person skilled in the art to the invention claimed in the claims.

Therefore, the invention defined in claims 1 - 15 is novel and considered to involve an inventive step. It is also considered to be industrially applicable.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 00/01842

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: G07F 7/08, G07F 7/10
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: G07F, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5878337 A (JOAO ET AL), 2 March 1999 (02.03.99), abstract --	1-15
A	US 5708422 A (G.E.BLONDER ET AL), 13 January 1998 (13.01.98), abstract --	1-15
A	WO 9945693 A1 (WALKER ASSET MANAGEMENT LTD.), 10 Sept 1999 (10.09.99), abstract --	1-15
A	US 5416306 A (T.IMAHATA), 16 May 1995 (16.05.95), abstract -- --------	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2001	23 -01- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Gordana Ninkovic´ / itw Telephone No. +46 8 782 25 00

PCT
REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

For receiving Office use only

International Application No. PCT/SE 0 0 / 0 1 8 4 2

International Filing Date 2 2 -09- 2000

The Swedish Patent Office
PCT International Application

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired)(12 characters maximum)* 2006796

Box No. I TITLE OF INVENTION

METHOD AND SYSTEM FOR VERIFICATION OF A SERVICE REQUEST

Box No. II APPLICANT

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

AB TRYGGIT
Torred 4164
SE-429 34 KULLAVIK
SWEDEN

☐ This person is also inventor.

Telephone No.

Facsimile No.

Teleprinter No.

State *(that is, country)* of nationality: SE

State *(that is, country)* of residence: SE

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Box No. III FURTHER APPLICANT(S) AND/OR /FURTHER INVENTOR(S)

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

BRYNIELSSON, Thore
Torred 4164
SE-429 34 KULLAVIK
SWEDEN

This person is:

☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below.)*

State *(that is, country)* of nationality: SE

State *(that is, country)* of residence: SE

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on a continuation sheet

Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

AWAPATENT AB
Box 11394
SE-404 28 GÖTEBORG
SWEDEN

Telephone No.
+46 31 63 02 00

Facsimile No.
+46 31 63 02 63

Teleprinter No.

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent

Box No. V DESIGNATION OF STATES

The following designations are hereby made under Rule 4.9(a) *(mark the applicable check-boxes; at least one must be marked)*:

Regional Patent

☒ **AP** **ARIPO Patent: GH** Ghana, **GM** Gambia, **KE** Kenya, **LS** Lesotho, **MW** Malawi, **MZ** Mozambique, **SD** Sudan, **SL** Sierra Leone, **SZ** Swaziland, **TZ** United Republic of Tanzania, **UG** Uganda, **ZW** Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT

☒ **EA** **Eurasian Patent: AM** Armenia, **AZ** Azerbaijan, **BY** Belarus, **KG** Kyrgyzstan, **KZ** Kazakhstan, **MD** Republic of Moldova, **RU** Russian Federation, **TJ** Tajikistan, **TM** Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT

☒ **EP** **European Patent: AT** Austria, **BE** Belgium, **CH and LI** Switzerland and Liechtenstein, **CY** Cyprus, **DE** Germany, **DK** Denmark, **ES** Spain, **FI** Finland, **FR** France, **GB** United Kingdom, **GR** Greece, **IE** Ireland, **IT** Italy, **LU** Luxembourg, **MC** Monaco, **NL** Netherlands, **PT** Portugal, **SE** Sweden, and any other State which is a Contracting State of the European Patent Convention and of the PCT

☒ **OA** **OAPI Patent: BF** Burkina Faso, **BJ** Benin, **CF** Central African Republic, **CG** Congo, **CI** Côte d'Ivoire, **CM** Cameroon, **GA** Gabon, **GN** Guinea, **GW** Guinea-Bissau, **ML** Mali, **MR** Mauritania, **NE** Niger, **SN** Senegal, **TD** Chad, **TG** Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)*

National Patent *(if other kind of protection or treatment desired, specify on dotted line)*:

☒	**AE**	United Arab Emirates	☒	**LC**	Saint Lucia
☒	**AG**	Antigua and Barbuda	☒	**LK**	Sri Lanka
☒	**AL**	Albania	☒	**LR**	Liberia
☒	**AM**	Armenia	☒	**LS**	Lesotho
☒	**AT**	Austria +Utility Model	☒	**LT**	Lithuania
☒	**AU**	Australia	☒	**LU**	Luxembourg
☒	**AZ**	Azerbaijan	☒	**LV**	Latvia
☒	**BA**	Bosnia and Herzegovina	☒	**MA**	Morocco
☒	**BB**	Barbados	☒	**MD**	Republic of Moldova
☒	**BG**	Bulgaria	☒	**MG**	Madagascar
☒	**BR**	Brazil	☒	**MK**	The former Yugoslav Republic of Macedonia
☒	**BY**	Belarus	☒	**MN**	Mongolia
☒	**BZ**	Belize	☒	**MW**	Malawi
☒	**CA**	Canada	☒	**MX**	Mexico
☒	**CH and LI**	Switzerland and Liechtenstein	☒	**MZ**	Mozambique
☒	**CN**	China	☒	**NO**	Norway
☒	**CR**	Costa Rica	☒	**NZ**	New Zealand
☒	**CU**	Cuba	☒	**PL**	Poland
☒	**CZ**	Czech Republic +Utility Model	☒	**PT**	Portugal
☒	**DE**	Germany +Utility Model	☒	**RO**	Romania
☒	**DK**	Denmark +Utility Model	☒	**RU**	Russian Federation
☒	**DM**	Dominica	☒	**SD**	Sudan
☒	**DZ**	Algeria	☒	**SE**	Sweden
☒	**EE**	Estonia +Utility Model	☒	**SG**	Singapore
☒	**ES**	Spain	☒	**SI**	Slovenia
☒	**FI**	Finland +Utility Model	☒	**SK**	Slovakia +Utility Model
☒	**GB**	United Kingdom	☒	**SL**	Sierra Leone
☒	**GD**	Grenada	☒	**TJ**	Tajikistan
☒	**GE**	Georgia	☒	**TM**	Turkmenistan
☒	**GH**	Ghana	☒	**TR**	Turkey
☒	**GM**	Gambia	☒	**TT**	Trinidad and Tobago
☒	**HR**	Croatia	☒	**TZ**	United Republic of Tanzania
☒	**HU**	Hungary	☒	**UA**	Ukraine
☒	**ID**	Indonesia	☒	**UG**	Uganda
☒	**IL**	Israel	☒	**US**	United States of America
☒	**IN**	India	☒	**UZ**	Uzbekistan
☒	**IS**	Iceland	☒	**VN**	Viet Nam
☒	**JP**	Japan	☒	**YU**	Yugoslavia
☒	**KE**	Kenya	☒	**ZA**	South Africa
☒	**KG**	Kyrgyzstan	☒	**ZW**	Zimbabwe
☒	**KP**	Democratic People's Republic of Korea			
☒	**KR**	Republic of Korea +Utility Model			
☒	**KZ**	Kazakhstan			

Check-boxes reserved for designating States which have become party to the PCT after issuance of this sheet:

☐ ☐

Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

Sheet No. 3

Box No. VI PRIORITY CLAIM ☐ Further priority claims are indicated in the Supplement Box.

Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is: national application: country	regional application:* regional Office	international application: receiving Office
item (1) 1 October 1999	9903575-0	SWEDEN		
item (2)				
item (3)				

☒ The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of the present international application is the receiving Office)* identified above as item(s): 1

** Where the earlier application is an ARIPO application, it is mandatory to indicate in the Supplemental Box at least one country party to the Paris Convention for the Protection of Industrial Property for which that earlier application was filed (Rule 4.10(b)(ii)). See Supplemental Box.*

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) *(If two or more International Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):*

ISA / SE

Request to use results of earlier search; reference to that search *(if an earlier search has been carried out by or requested from the International Searching Authority):*

Date *(day/month/year)*	Number	Country *(or regional Office)*
15 December 1999	SE99/01592	Sweden

Box No. VIII CHECK LIST; LANGUAGE OF FILING

This international application contains the following **number of sheets:**

request	: 3
description (excluding sequence listing part)	: 23
claims	: 4
abstract	: 1
drawings	: 6
sequence listing part of description	:
Total number of sheets	: 37

This international application is **accompanied by** the item(s) marked below:

1. ☒ fee calculation sheet
2. ☒ separate signed power of attorney
3. ☐ copy of general power of attorney; reference No., if any:
4. ☐ statement explaining lack of signature
5. ☐ priority document(s) identified in Box No. VI as item(s):
6. ☐ translation of international applications into (language):
7. ☐ separate indications concerning deposited microorganism or other biological material
8. ☐ nucleotide and/or amino acid sequence listning in computer readable form
9. ☒ other (specify): Subauthorization, Copy of ITS-report

Figure of the drawings which should accompany the abstract: 5a

Language of filing of the international application: Swedish

Box No. IX SIGNATURE OF APPLICANT OR AGENT

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).

Göteborg, 21 September 2000

Fabian Edlund

Fabian Edlund
Authorized Representative, Awapatent AB

For receiving Office use only

1. Date of actual receipt of the Purported international application: 22-09-2000		2. Drawings: ☒ received: ☐ not received:
3. Corrected date of actual receipt due to later but Timely received papers or drawings completing the purported international application:		
4. Date of timely receipt of the required Corrections under PCT Article 11(2):		
5. International Searching Authority (if two or more are competent): ISA/SE	6. ☐ Transmittal of search copy delayed until search fee is paid.	

For International Bureau use only

Date of receipt of the record copy by the International Bureau: 10 NOVEMBER 2000 (10.11.00)

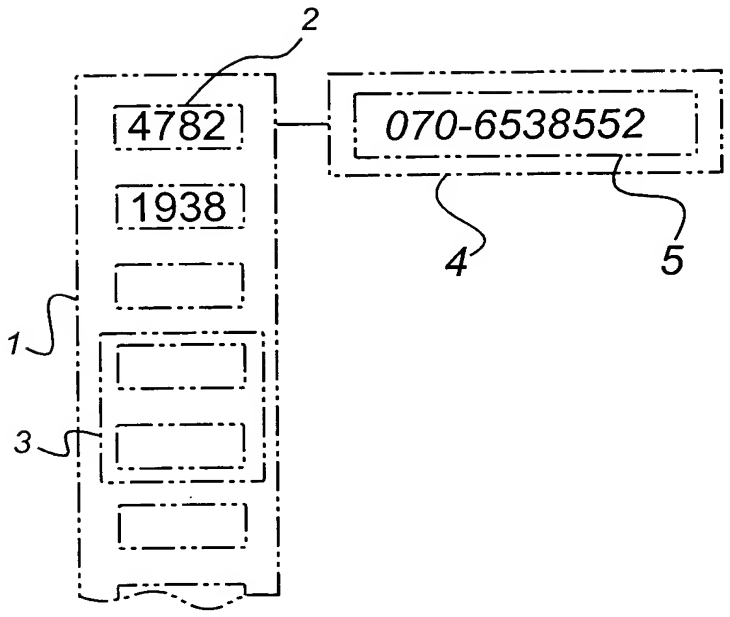


Fig 1

Kodord i mobil och i ID-databas innan det aktuella uppdraget påbörjats:

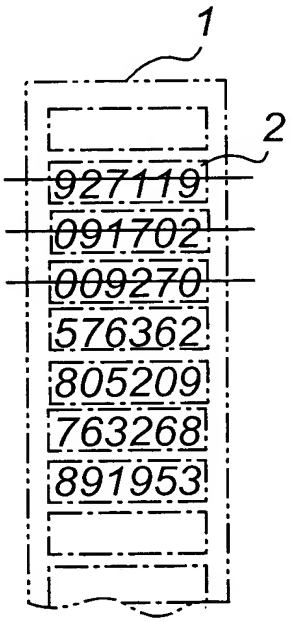


Fig 1b

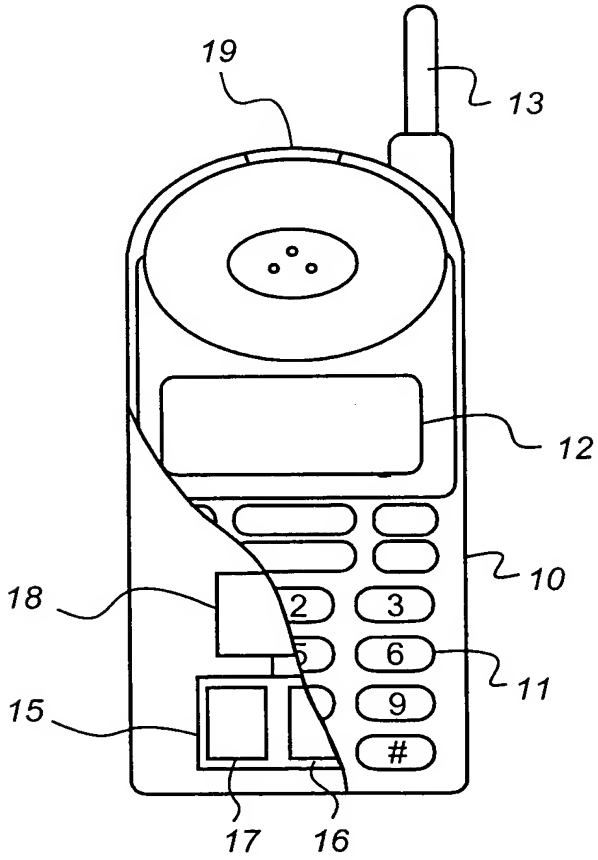


Fig 2

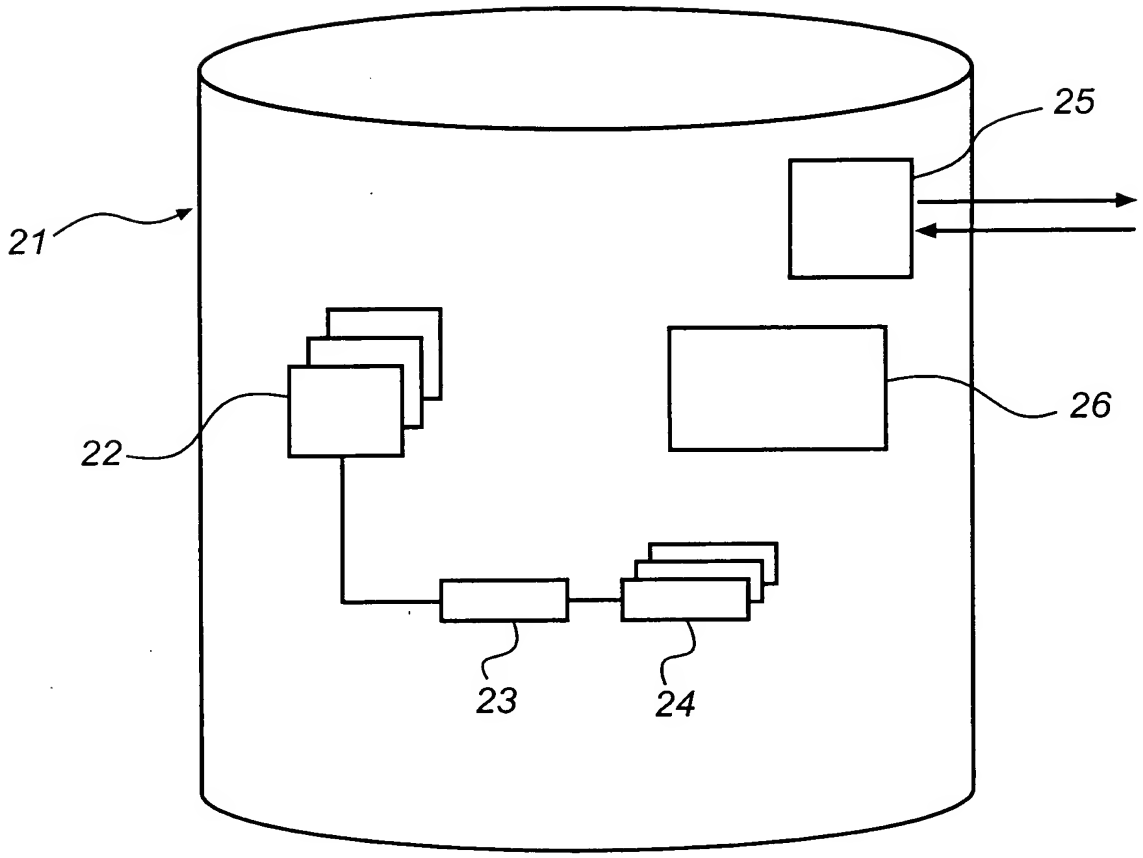


Fig 3

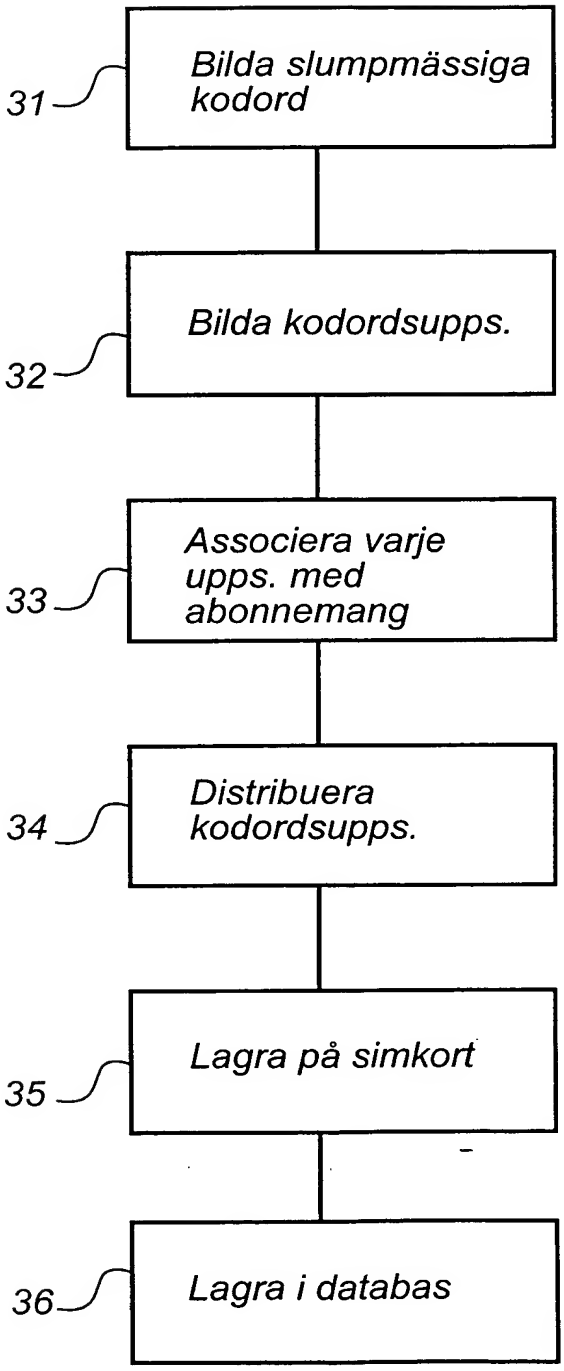

31
Bilda slumpmässiga kodord
32
Bilda kodordsupps.
33
Associera varje upps. med abonnemang
34
Distribuera kodordsupps.
35
Lagra på simkort
36
Lagra i databas

Fig 4

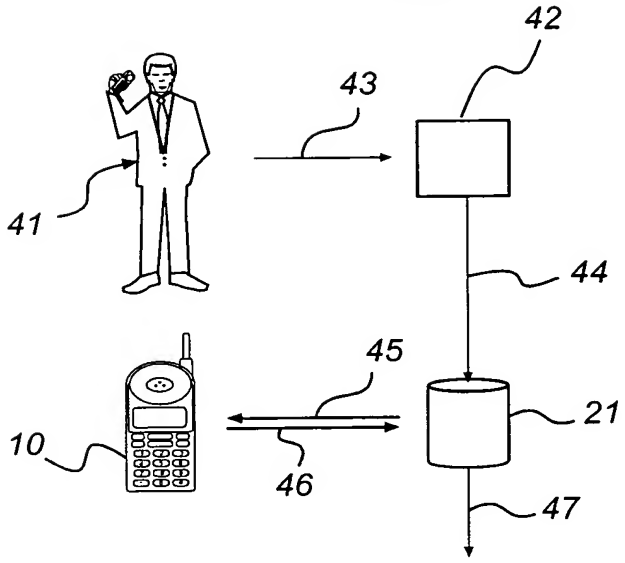


Fig 5a

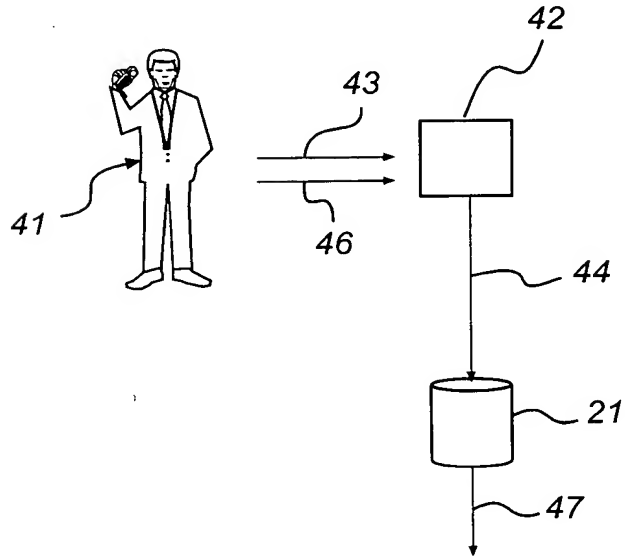


Fig 5b

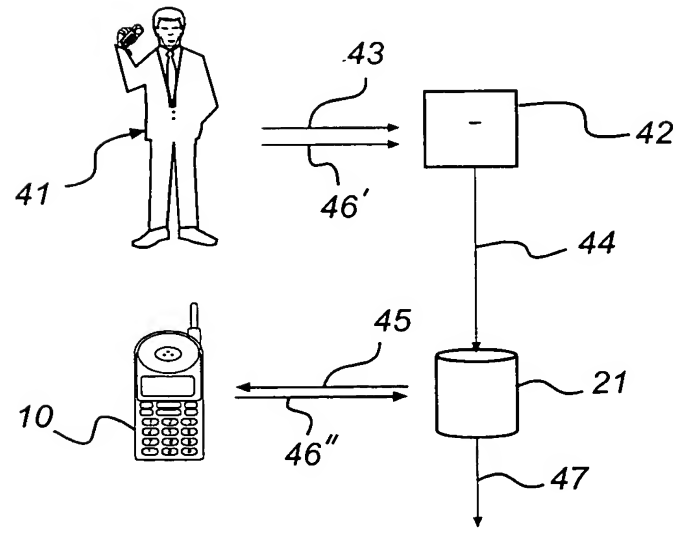


Fig 5c

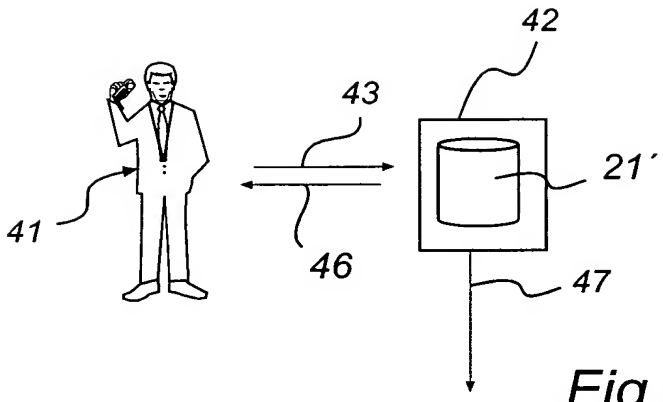


Fig 5d

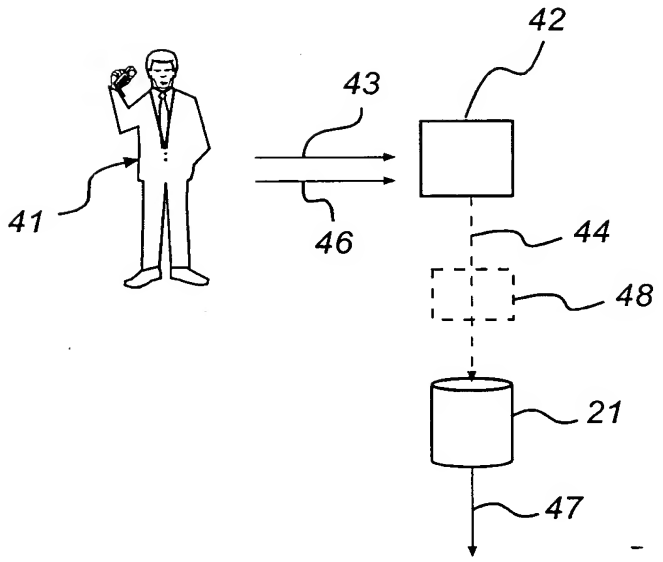


Fig 5e

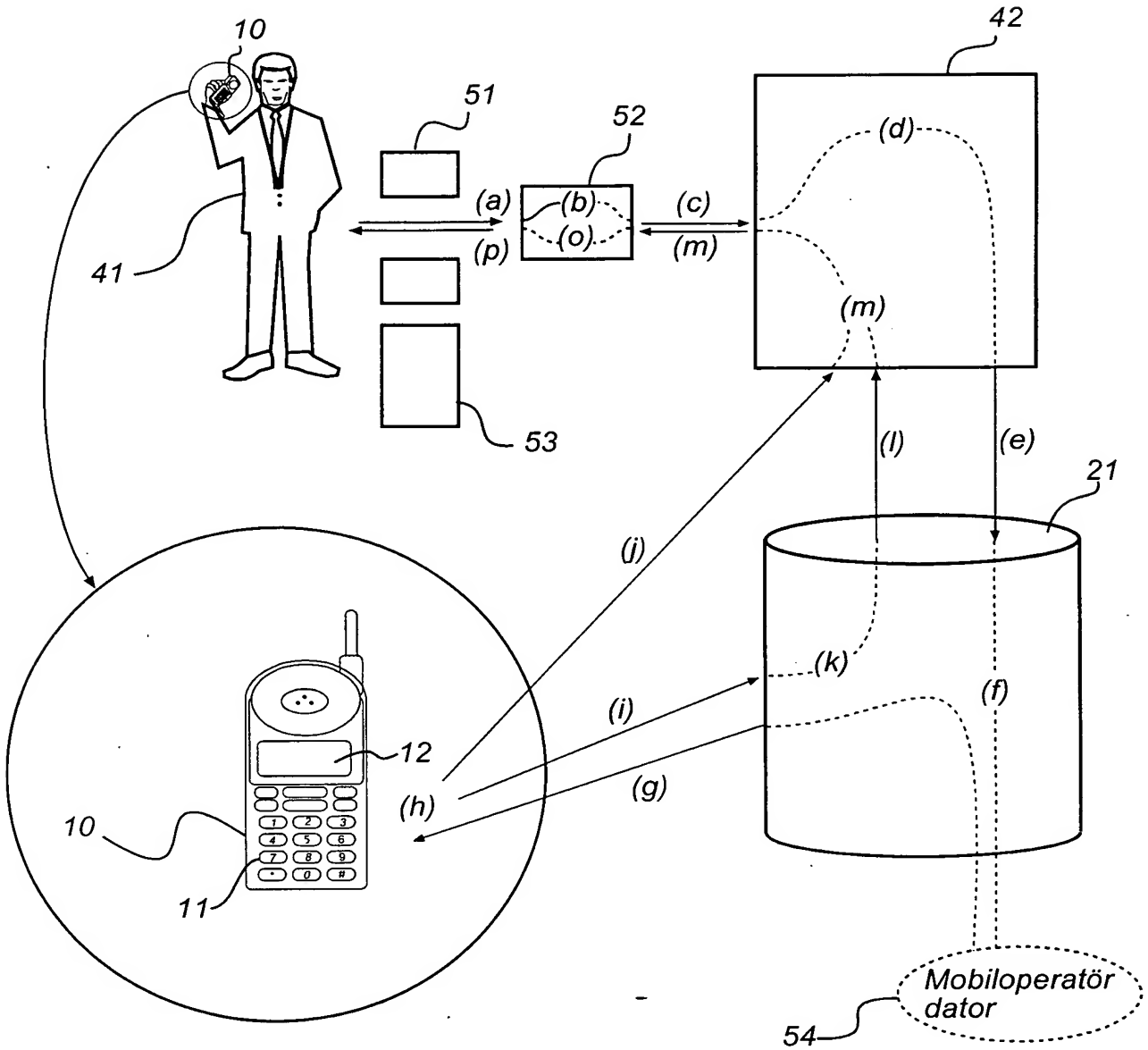

10
42
51
52
(d)
(a)
(b)
(c)
(p)
(o)
(m)
41
(m)
53
(l)
(e)
21
(j)
(k)
(f)
(i)
12
(h)
(g)
10
11
Mobiloperatör
dator
54

Fig 6

AWAPATENT AB
Kontor/Handläggare
Göteborg/Fabian Johnsson/LRH

TRYGGIT AB
Ansökningsnr

Vår referens
[redacted]-2006796

METOD OCH SYSTEM FÖR VERIFIERING AV TJÄNSTEBESTÄLLNING

Tekniskt område

Föreliggande uppfinning avser en metod och ett system för att verifiera uppdrag från en beställare till en tjänsteleverantör.

Teknisk bakgrund

Vid köp med kredit- eller betalkort i handeln finns ett ständigt problem att bestämma användarens identitet. Varje kort har vanligtvis en specifik kod, exempelvis en fyrställig sifferkod, vilken i vissa butiker kan matas in i samband med köpet. Detta är emellertid ingen speciellt attraktiv lösning för en person med ett tiotal kort, vardera med en specifik kod. I exempelvis restauranger tillämpas ofta systemet att gästen skriver under en bekräftelse av transaktionen, vilken underskrift fungerar som en efterkontroll om betalningen ifrågasätts. Detta innebär att kortets ägare endast i efterhand märker om någon använt kortet utan ägarens vetskap. Det förekommer till och med att restaurangens personal i bedrägligt syfte belastar ett kort med flera transaktioner under den tid de ensamma har tillgång till kortet. Ofta räcker det att en bedragare kommer över kortnumret, för att bedragaren sedan ska kunna använda detta kort vid ett senare tillfälle.

Enligt en känd teknik, avsedd för situationer där en kund har återkommande kontakt med exempelvis en bank, har kunden en skrapbar lista med koder. Banken har tillgång till samma lista, exempelvis lagrad i sitt datorsystem. Varje gång kunden beställer en transaktion, exempelvis via telefon, skrapar han fram ett nummer som anges. Numret kontrolleras mot bankens lista, varigenom säkerställs att kunden är den han utger sig för att vara, eller åtminstone har kommit över den aktuella skraplistan.

I kända system för säkra transaktioner på exempelvis Internet, förkommer en liten dosa, som användaren måste ha tillgång till vid transaktionstillfället. Koder utväxlas mellan datorn och dosan för att säkerställa att användaren verkligen har tillgång till dosan. Denna teknik används framförallt i samband med banktjänster på Internet, då en användare relativt ofta utnyttjar tjänsten.

Lösningen med den personliga dosan uppvisar dock två problem:

För det första är det möjligt för en insatt fackman att kopiera elektroniken, exempelvis ROM-minnet, i en dosa som han har tillgång till en kort stund. Dosan kan sedan återlämnas till den intet ont anande ägaren. Ingen möjlighet finns sedan för datorsystemet att avgöra om det är ägaren eller bedragaren som beställer en transaktion.

För det andra är en dosa specifik för en tjänsteleverantör, vilket för en användare av flera tjänster innebär att ett flertal dosor ska medföras. Risken finns då att användaren har glömt den dosa som han för tillfället behöver. Vidare minskar användarens möjligheter att hålla samtliga dosor under uppsikt, och en bedragare kan lätt använda en stulen dosa, eller kopiera en "lånad" dosa, utan att användaren hinner sakna dosan.

När kontokort används för betalningar över Internet, är det oftast endast kontokortsnumret som fungerar som kontroll. Kontokortnumret kan visserligen krypteras, men om krypteringen knäcks kan en bedragare handla relativt obehindrat tills användaren får en räkning, vanligtvis i slutet av månaden. Visserligen skulle dosor av ovan nämnt slag kunna utnyttjas för att förbättra säkerheten, men ovannämnda problem med kopiering av dosan, respektive behovet av flera dosor kvarstår då naturligtvis.

Vissa tjänsteleverantörer har system på Internet där man först måste anmäla sig som kund, och först därefter kan handla med sitt kontokort. Dessa system har dock liksom dosan den nackdel att de är specifika för varje tjänsteleverantör, och användaren får därmed en mycket

krånglig tillvaro i kontakten med flera olika tjänsteleverantörer.

Andra mycket vanliga tjänst med behov av verifiering av en användare är inloggning i datorsystem, samt inpassering i säkerhetsklassade lokaler. Dessa system bygger nästan uteslutande på angivande av ett användar-ID tillsammans med en kod eller ett lösenord, vilket i vissa system bytes enligt bestämda rutiner, respektive på passerkort med tillhörande kod. Helt allmänt kan konstateras att det i vårt samhälle förekommer en uppsjö av koder, vilka för en människa är svåra att hålla i minnet. Frestelsen är därför stor att notera koderna någonstans, varvid säkerheten minskar.

Att kombinera angivandet av en kod med en dosa, vilken rent fysiskt måste finnas till hands förbättrar säkerheten, men till priset av en mängd dosor. Denna teknik är därför knappast någon universell lösning på ovanstående problematik.

Behov finns därför av ett enhetligt system som skulle kunna användas vid flera olika typer av tjänstebeställningar, genom vilket användarens legitimitet kan verifieras på ett enkelt sätt.

Definitioner

I den följande beskrivningen förekommer ett antal termer, vilka här definieras.

Med termen "uppdrag" avses helt allmänt en tjänst eller service som en person önskar utförd av en leverantör. Exempelvis kan ett uppdrag vara en ekonomisk transaktion, som utförs av en bank eller liknande, men ett uppdrag kan också vara en begäran att bli insläppt i en byggnad eller inloggad i ett datorsystem. Beställningen av detta uppdrag refereras till som en "tjänstebeställning".

Med termen "tjänsteleverantör" avses både företaget som utför uppdraget (exempelvis en bank, ett kontokortföretag eller ett säkerhetsbolag), och den utrustning som

utför uppdraget (exempelvis ett portlås, en bankomat, eller ett datorsystem vid inloggning).

"Beställaren" är personen som begär uppdraget av tjänsteleverantören, och beställaren och tjänsteleverantören är i följande beskrivning tillika användare av metoden och systemet enligt uppfinningen.

Termen "databas" avser såväl den minnesenhet där data lagras som den mjukvara som hanterar datamängder och utför operationer exempelvis i syfte att jämföra datamängder.

Med "mobiltelefon" avses en bärbar telefon, exempelvis en GSM-telefon eller liknande. Även eventuella framtida bärbara telefoner innefattas naturligtvis av termen.

Uppfinningens syften

Ett första syfte med föreliggande uppfinning är att lösa ovanstående problem, och göra det möjligt att verifiera en beställare av en tjänst på ett tillfredsställande sätt.

Ett andra syfte med uppfinningen är att göra det möjligt att verifiera en beställare av en tjänst, vilken metod är universell, och enkelt kan utnyttjas av flera tjänsteleverantörer utan behov av för leverantören specifik utrustning.

Sammanfattning av uppfinningen

Dessa syften uppnås enligt uppfinningen med en metod och ett system enligt de självständiga patentkraven 1, 13 och 14.

Enligt uppfinningen finns således för varje beställare två identiska uppsättningar kodord, av vilka den ena finns lagrad på en minneskrets i en mobiltelefon, och den andra finns lagrad i en databas. Verifikationen av beställaren utförs genom att mobilteleabonnemanget identifieras, ett kodord utvinns ur minneskretsen, och kodordet kontrolleras mot den kodordsuppsättning i databasen som direkt eller indirekt är associerad med mobilteleabonne-

manget. Den inbördes ordningen mellan ovannämnda moment kan naturligtvis vara annorlunda, exempelvis kan kodordet utvinnas ur minneskretsen innan mobilteleabonnemanget identifieras.

En fördel med systemet och metoden enligt uppfinningen i förhållande till känd teknik är att kodorden är av engångskaraktär i kombination med att ingen förutsägbar algoritm utnyttjas för att härleda nästa kodord. För att känna till kodorden i en uppsättning måste mobiltelefonens minneskrets stjälas rent fysiskt eller kopieras på exempelvis elektronisk väg.

Vidare är metoden och systemet enligt uppfinningen användbara av ett obegränsat antal tjänsteleverantörer. Det enda som erfordras av tjänsteleverantören är utrustning för att koppla upp sig mot databasen och överföra kodordet och identiteten, och att motta resultatet av kontrollen. Detta innebär vidare att användaren genom att spärra sitt mobilteleabonnemang i databasen enkelt kan spärra samtliga tjänster som utnyttjar systemet. Ett alternativ är att tjänsteleverantören själv äger databasen, eller en delmängd därav.

En ytterligare fördel är att systemet är användbart helt parallellt med och oberoende av befintliga säkerhetssystem. Således kan varje tjänsteleverantör på egen hand välja om den vill ansluta sig till systemet, och därigenom förbättra säkerheten i sitt befintliga system.

Kodordet utvinns företrädesvis ur minneskretsen enligt en förutbestämd ordning, vilket ytterligare förbättrar verifikationens säkerhet. Förutom att kodordet kontrolleras tillhöra den kodordsuppsättning som är associerad med den uppgivna identiteten, kontrolleras också att det är rätt kodord inom uppsättningen.

I minneskretsen kan markeras när ett kodord har använts, och en liknande markering kan utföras i databasen. Härigenom säkerställs att minneskretsen och databasen har samma uppfattning om var i den förutbestämda ordningen nästa kodord ska hämtas. Man förhindrar alltså att min-

neskretsen och databasen kommer "ur fas". Detta system kan liknas vid att beställaren bär med sig en skrapbar lista med kodord. För att använda ett kodord skrapas det fram, varvid tjänsteleverantören skrapar fram motsvarande kodord i sin lista och jämför de båda. För att beställningen ska accepteras måste rätt lista användas, och dessutom rätt kodord på listan.

En konsekvens av detta förfarande är att en bedragare som i lönndom kommit över en persons kodordsuppsättning, exempelvis genom att på elektronisk väg kopierat minneskretsen, endast kommer att kunna utnyttja minneskretsen om inte personen dessförinnan gjort en beställning, och därmed använt nästa kodord. Om bedragaren verkligen lyckas genomföra en beställning, kommer bedrägeriet att upptäckas senast nästa gång personen ska göra en beställning, eftersom det kodord som då anges inte accepteras. Mobilabonnemanget kan då spärras, varvid skadan minimeras. Jämför med en i lönndom kopierad säkerhetsdosa enligt känd teknik, som kan användas av en bedragare tills ägaren får ett uppseendeväckande kontouppdrag eller liknande.

Steget att identifiera mobilteleabonnemanget innefattar företrädesvis stegen att bestämma beställarens identitet, och att utifrån beställarens identitet identifiera mobilteleabonnemanget. Beställarens identitet kan utgöras av lämplig data, exempelvis ett personnummer, ett kontokortsnummer eller ett mobiltelefonnummer. Begreppet identitet betecknar egentligen enbart en direkt koppling till en person, och den data som representerar identiteten kan eventuellt utbytas. Sålunda kan identiteten från beställaren till tjänsteleverantören anges i form av exempelvis ett bank- eller passerskortsnummer med tillhörande kod, eller ett användar-ID med tillhörande kod, och från tjänsteleverantören till databasen anges i form av ett mobiltelefonnummer eller ett förutbestämt ID-nummer. Databasen måste dock kunna koppla ihop den mottagna identiteten med en bestämd kodordsuppsättning, normalt via

mobiltelefonnumret, för att därigenom kunna kontrollera att det angivna kodordet har utvunnits från rätt minneskrets.

Enligt en föredragen utföringsform skickas en begäran till beställaren att uppge ett kodord. Beställaren kan alltså beställa en tjänst på vanligt sätt, varpå tjänsteleverantören som en ytterligare säkerhetsåtgärd begär ett kodord, som beställaren då utvinner ur mobiltelefonen. Tjänsteleverantören har lämpligen information om vilka av dess kunder som är anslutna till systemet enligt uppfinningen, och skickar i förekommande fall en förfrågan till databasen. Databasen skickar därefter en begäran till beställaren att uppge ett kodord.

Begäran kan skickas via telenätet till mobiltelefonen och kodordet kan överförs från mobiltelefonen till databasen via telenätet. Lämpligen accepterar beställaren att kodordet skickas genom lämpliga knapptryckningar på mobiltelefonen. Eftersom härigenom två separata kommunikationsvägar utnyttjas, för det första en väg mellan tjänsteleverantören och databasen, och för det andra mellan databasen och mobiltelefonen, förbättras säkerheten ytterligare. En bedragare som uppfångat och förvanskat information längs den första kommunikationsvägen, har ingen möjlighet att förutse vilket mobilteleabonnemang eller basstation som nästa led i verifikationsprocessen kommer att utnyttja.

Begäran som skickas till mobiltelefonen, som exempelvis är ett SMS-meddelande eller liknande, kan innehålla information om transaktionen. Detta kan vara fördelaktigt exempelvis i en situation där kortet dragits i kortterminalen, och godkänts av kortföretaget, men där transaktionens belopp ännu inte fastställts. En bedragare skulle då, när hela verifikationen utförts, kunna ange ett felaktigt belopp, och därmed belasta beställarens konto för mycket. Genom ett SMS-meddelande enligt ovan skulle detta upptäckas av beställaren, som alltså får in-

formation om den bedrägliga beställningen till sin mobiltelefon, och då kan förneka transaktionen.

Genom att mobiltelefonen kontaktas direkt ges en möjlighet för en användare att upptäcka ett pågående bedrägeri. Användaren kan då omedelbart spärra mobilabonnemanget, eller spärra det kort eller den tjänst som är utsatt för bedrägeri. Antag att någon stulit eller kopierat en persons kontokort, och dessutom lyckats komma över nästa kod på personens minneskrets. När kortet används, och en transaktion godkännes av databasen, skickas ett meddelande till personens mobiltelefon, varpå personen får kännedom om att någon använt ett av kodorden på minneskretsen. En möjlighet är vidare att dröja med kodordsbegäran till beställaren en bestämd tid, eller att tillämpa två bekräftelser, åtskilda i tiden. Detta skulle utesluta att en bedragare använder en mobiltelefon som sedan lämnas tillbaka, utan att ägaren märker det. Fördröjningstiden kan anpassas så att mobiltelefonens ägare hinner sakna den och spärra den innan begäran om kodord skickas till mobiltelefonen och därmed verifierar beställningen.

Samtidigt möjliggör denna metod att en beställare kan låta en tredje person använda beställarens kort för en bestämd tjänst, exempelvis att köpa en vara. Beställaren får oavsett var han befinner sig, information om köpet på sin mobiltelefon, och gör den definitiva bekräftelsen via sin mobiltelefon.

Speciellt vid tjänstebeställningar via Internet är det fördelaktigt med en begäran från databasen eller tjänsteleverantören direkt till mobiltelefonen, eftersom all information som överförs via Internet är mer eller mindre åtkomlig för andra. Ett SMS-meddelande till beställarens telefon blir därför en utmärkt kvittens på att transaktionen är korrekt.

Enligt en annan utföringsform av uppfinningen överförs beställarens identitet och det ur minneskretsen ut-

vunna kodordet till tjänsteleverantören, mobilteleabonnemanget som är associerat till beställaren identifieras av tjänsteleverantören, och kodordet och mobilteleabonnemangets identitet överförs till databasen av tjänsteleverantören. Med detta förfarande kan beställaren alltså direkt i samband med beställningen överföra både sin identitet och ett kodord till tjänsteleverantören. Identifieringen av mobilteleabonnemanget utförs därefter antingen av tjänsteleverantören eller av databasen.

Enligt en ytterligare utföringsform av uppfinningen utvinns ett andra kodord från minneskretsen och överförs till databasen, för att ytterligare verifiera uppdraget. Kodorden i uppsättningen kan vara associerade till varandra i grupper med olika antal kodord, för att användas vid olika typer av tjänstebeställningar med olika säkerhetsnivå.

Det första kodordet kan överföras från beställaren till databasen, eventuellt via tjänsteleverantören, varpå databasen skickar en begäran till beställaren att uppge ett andra kodord, och slutligen det andra kodordet överförs från beställaren till databasen. Begäran till beställaren kan ske på samma sätt som den ovan beskrivna begäran. En möjlighet är alltså att beställaren direkt till mobiltelefonen, får två på varandra följande begäran om att överföra ett kodord. En annan möjlighet är att beställaren först anger ett kodord direkt i samband med beställningen, varpå beställaren därefter får en begäran om att ange ett ytterligare kodord. Fler möjligheter är naturligtvis möjliga, och speciellt kan även mobiltelefonens PIN-kod utnyttjas som ett sätt att ytterligare höja säkerheten i verifikationen.

Enligt en utföringsform av uppfinningen lagras i databasen även positionsangivelser som är associerade med mobilteleabonnemanget. Vid verifikationen lokaliseras minneskretsen, och den erhållna positionen kan jämföras med de i databasen lagrade positionsangivelserna. Detta förfarande kan utnyttjas för att geografiskt begränsa var

en beställare kan utföra vissa typer av tjänster. Exempelvis kan köp över ett visst belopp vara begränsade till ett fåtal, förutbestämda platser, vilket ytterligare ökar säkerheten. Denna geografiska kontroll kan också vara tillämpbart vid inloggning i ett datorsystem, som kanske endast är tillåten från arbetsplatsen eller hemifrån. Alternativt kan en positionsangivelse i databasen vara en IP-adress, varigenom inloggningsförfarande eller Internettransaktioner kan begränsas till en bestämd dator, utan att denna information finns tillgänglig hos tjänsteleverantören eller någonstans på Internet.

Kort beskrivning av ritningarna

Föreliggande uppfinning kommer i det följande att beskrivas närmare under hänvisning till bifogade ritningar, vilka i exemplifierande syfte visar föredragna utföringsformer av uppfinningen.

Fig 1a-b visar två kodordsuppsättningar enligt uppfinningen.

Fig 2 visar en mobiltelefon enligt uppfinningen.

Fig 3 visar en databas enligt uppfinningen.

Fig 4 visar hur kodordsuppsättningar enligt fig 1 framtages och lagras.

Fig 5a-e visar fem föredragna utföringsformer av metoden enligt uppfinningen.

Fig 6 visar en mer detaljerad illustration av metoden enligt uppfinningen.

Beskrivning av föredragna utföringsformer

I fig 1a-b visas två exempel på en kodordsuppsättning 1, som består av ett flertal koder 2 i form av fyr- eller sexställiga sifferkombinationer. Dessa sifferkombinationer är helt slumpmässigt framtagna, och uppvisar inget härledbart samband, vare sig avseende sammansättning eller ordningsföljd. Koderna kan vara ordnade i grupper 3, med två eller flera koder 2 i varje grupp.

Eftersom varje kod i sig är helt oberoende av de övriga finns inget hinder mot att en sifferkombination förekommer flera gånger i samma uppsättning, eller till och med i samma grupp.

Kodordsuppsättningen 1 är associerad med en identitet 4, som direkt eller indirekt är förknippad med ett mobilteleabonnemang. I det visade exemplet utgörs identiteten av ett mobiltelefonnummer 5.

Mobiltelefonen 10 som schematiskt visas i fig 2 har på känt vis en knappsats 11, en display 12, samt en mottagare/sändare 13. Mobiltelefonen har vidare en minneskrets 15, exempelvis ett SIM-kort eller motsvarande smart-card, vilken innehåller information 16 om mobilteleabonnemanget. Exempelvis kan ett SIM-kort innehålla information om abonnemangets telefonnummer, och om hur mycket kredit som återstår på ägarens konto hos mobiltjänstleverantören. Minneskretsen 15 är vidare enligt uppfinningen försedd med den kodordsuppsättning 17 som är associerad med abonnemanget.

SIM-kortet kan förses med ett abonnemangs-ID och en kodordsuppsättning innan det levereras till en återförsäljare under noggrann sekretess, exempelvis genom någon form av sigillförslutning. Användaren som köper eller på annat sätt kommer över SIM-kortet kontrollerar att sigillet inte är brutet och anordnar därefter SIM-kortet i sin mobiltelefon för att kunna använda denna.

Den i fig 2 visade mobiltelefonen är vidare försedd med organ, exempelvis en mjukvara 18, för att från minneskretsen 15 utvinna ett kodord från kodordsuppsättningen 17, och sända detta medelst mobiltelekommunikation, exempelvis i ett SMS-meddelande. En mjukvara med denna funktionalitet kan utvecklas av en fackman på området. Mjukvaran 18 kan också överföra ett kodord via en kommunikationsport 19, såsom en seriell eller parallell dataöverföringsport, eller infraröd port. Vidare kan ett utvunnet kodord visas på displayen 12.

Mjukvaran 18 är vidare anordnad att motta ett kodord och jämföra kodordet med kodordsuppsättningen i minneskretsen. Kodordet kan inmatas medelst knappsatsen 11, eller också mottas medelst mobiltelekommunikation direkt till mobiltelefonens mottagare 13, exempelvis genom att mobiltelefonen mottar ett SMS-meddelande.

Det är lämpligt att mobiltelefonen kan försättas i ett sov-läge, där inga telefonsamtal tas emot, men där SMS-meddelanden kan mottas och sändas. Denna funktion kan utvecklas av en fackman på området.

I databasen 21, som visas i fig 3, är ett flertal kodordsuppsättningar 22 lagrade, vilka vardera har en identitet 23 som är associerad till ett mobilteleabonnemang, vars motsvarande SIM-kort innefattar en identisk kodordsuppsättning.

Varje uppsättning 22 kan vidare vara kopplad till en eller flera positionsangivelser 24. Positionsangivelserna kan exempelvis vara ställen på vilka beställaren angivit att han vill kunna utföra en viss typ av beställningar.

Databasen 21 är vidare försedd med kommunikationsorgan 25 för att motta en förfrågan, samt meddela resultatet av verifikationen. Exempelvis kan kommunikationsorganet 25 utgöras av ett modem som är anordnat att kommunicera med tjänsteleverantören, till exempel att motta ett kodord och en identitet från tjänsteleverantören, samt att skicka en bekräftelse till tjänsteleverantören om att uppdraget är verifierat. Kommunikationsorganet 25 kan också vara anordnat att över mobiltelenätet, exempelvis via SMS-meddelanden, kommunicera med mobiltelefonen.

Vidare är databasen 21 försedd med organ, företrädesvis mjukvara 26, som är anordnad att utföra sökningar i databasen och att exempelvis verifiera att ett bestämt kodord återfinns i den kodordsuppsättning 22 i databasen som är associerad en bestämd identitet 23.

I fig 4 illustreras hur kodordsuppsättningar 1 bildas och lagras.

I ett helt fristående datorsystem slumpas sifferkombinationer fram enligt algoritmer som inte kan förutsägas utifrån (steg 31). Detta säkerställer att ingen kan förutse vilka kodord som ingår i en bestämd kodordsuppsättning, och kan enkelt åstadkommas av en fackman på området. Sifferkombinationerna grupperas i grupper och uppsättningar (steg 32), enligt algoritmer som i sig kan tillåtas vara kända utanför datorsystemet. Datorsystemet tillförs vidare en serie mobiltelefonnummer, vilka tillhandahålls av en mobilteletjänstleverantör, och associerar varje kodordsuppsättning med ett telefonnummer (steg 33).

Därefter distribueras uppsättningarna (steg 34) till företag som förser SIM-korten med information, där varje kodordsuppsättning lagras på ett SIM-kort (steg 35) som antingen före eller efter lagringen har tilldelats det mobiltelenummer som uppsättningen är associerad till.

Vidare distribueras (steg 34) uppsättningarna till databasen, där de också lagras (steg 36). Uppsättningarna kan lagras på åtkomstskyddade informationsbärare, exempelvis kodade och sigillförslutna CD-skivor, vilka distribueras på säkert sätt, exempelvis med kurir. Om datorsystemet som bildar uppsättningarna är anslutet till databasen, kan denna del av distributionen ske på säker elektronisk väg.

I fig 5a - e illustreras översiktligt fem olika varianter av hur verifikationen av ett uppdrag från en beställare 41 till en tjänsteleverantör 42 går till enligt uppfinningen. I samtliga fall har beställaren 41 en mobiltelefon 10 enligt fig 2.

Enligt metoden i fig 5a uppger beställaren först sin identitet 43 till tjänsteleverantören 42. Detta sker normalt i samband med beställningen av uppdraget, då beställaren exempelvis uppger ett användar-ID, ett kontokortsnummer eller annan information som för tjänsteleverantören identifierar beställaren.

Tjänsteleverantören har kännedom om vilka kunder som är anslutna till systemet enligt uppfinningen, och har möjlighet att associera ett mobilteleabonnemang till kundens identitet. Tjänsteleverantören 42 skickar en förfrågan 44 till databasen 21, och överför mobilteleabonnemangets identitet 23, vanligen i form av ett mobiltelenummer, men eventuellt i form av ett annan identifikation som är associerad med mobilteleabonnemanget, till databasen 21. Naturligtvis kan istället beställarens identitet 43 överföras till databasen 21, och det aktuella mobilteleabonnemanget identifieras av databasen.

Databasen skickar därefter en begäran 45 via telenätet till mobiltelefonen 10, exempelvis medelst ett SMS-meddelande eller liknande. Meddelandet 45 innehåller information om beställningen, som visas i displayen 12, så att beställaren kan kontrollera att beställningen är riktig. Om så är fallet kan beställaren bekräfta på lämpligt sätt, exempelvis med en dubbel knapptryckning på bestämd knapp i knapsatsen 11. Exempelvis kan beställaren till sin mobiltelefon få ett meddelande av typen "Kortköp $35 på BurgerKing. Tryck OK för att bekräfta", eller "Du loggar nu in på din arbetsplats. Tryck OK för att bekräfta". Beställaren trycker då på OK-knappen. En ytterligare bekräftelse av typen "Är du säker J/N" kan vara lämplig, som en extra kontroll. Mjukvaran 18 i mobiltelefonen hämtar då från SIM-kortet 15 nästa, ännu inte använda kod 46, och skickar denna från mobiltelefonen 10 till databasen 21. Samtidigt markeras det skickade kodordet som använt på SIM-kortet. Begäran 45 från databasen kan också innehålla ett kodord (ej visat), som av mobiltelefonens mjukvara 18 kontrolleras mot SIM-kortets 15 kodordsuppsättning 17.

En annan möjlighet är att databasen 21 kontaktar tjänsteleverantören 42, som i sin tur begär ett kodord från beställaren och returnerar detta till databasen 21.

När databasen 21 får kodordet 46 kan det jämföras med den uppsättning 22 som är associerad till mobiltele-

abonnemanget. Om kontrollen misslyckas, exempelvis beroende på att koden inte återfinns i kodordsuppsättningen i databasen som är associerad till mobiltelefonnumret, överförs information om detta till tjänsteleverantören, som kan vägra utföra tjänsten, exempelvis vägra tillträde till ett datorsystem eller stoppa en transaktion. Om kontrollen däremot är positiv, dvs den angivna koden är korrekt, överförs ett klartecken 47 till tjänsteleverantören 42, som då kan utföra tjänsten. Samtidigt markeras det mottagna kodordet som använt.

Enligt metoden som visas i fig 5b uppger beställaren 41 ett kodord 46 i samband med att beställaren uppger sin identitet 43 enligt ovan. Beställaren 41 kan exempelvis läsa av ett kodord 46 från mobiltelefonens 10 display 12, och överföra det till tjänsteleverantören 42. Alternativt kan en dataöverföringsport 19 hos mobiltelefonen användas för att överföra ett kodord till tjänsteleverantören.

Tjänsteleverantören skickar därefter en förfrågan 44 till databasen 21, och överför förutom identiteten enligt ovan, även kodordet 46. Databasen 21 kontrollerar kodordet enligt ovan, och skickar ett klartecken 47 till tjänsteleverantören 42.

Metoden som visas i fig 5c är egentligen en kombination av de två tidigare metoderna. Beställaren 41 uppger först ett kodord 46' i samband med beställningen enligt fig 5b, och mottar därefter en begäran 45 om ytterligare ett kodord 46'' enligt fig 5a.

För att ytterligare öka säkerheten kan mjukvaran 18 vara anordnad att vid vissa uppdrag, exempelvis köp över ett visst belopp, begära användarens PIN-kod för att utvinna och sända kodordet. Detta innebär att en bedragare som kommit över en påslagen mobiltelefon ändå är tvungen att känna till ägarens PIN-kod.

De i databasen lagrade positionsangivelserna kan också utnyttjas för att höja säkerheten. Den basstation som mobiltelefonen kommunicerar via kan relativt enkelt identifieras, och en jämförelse med de lagrade positions-

angivelserna kan utföras. Det kan också vara möjligt att i mobiltelefonen innefatta en GPS-navigator eller liknande, varvid mobiltelefonen kan kommunicera sin position mycket noggrant. Positionskontrollen skulle härvid kunna ske i två steg, först grovt, med avseende på basstation, och sedan mer noggrant, med avseende på longitud och latitud.

Metoden som visas i fig 5d kan ses som en variant av metoden som visas i fig 5b. Databasen 21' ägs här av tjänsteleverantören 42, varvid någon extern kommunikation ej behöver ske från tjänsteleverantören 42. Databasen 21' kan vara en delmängd av en större databas 21. Denna metod kan exempelvis användas när en person ska ges tillträde till ett skyddsobjekt, såsom en bil. Bilen har en databas 21' med ett antal kodord, och en användare kan enkelt identifieras med hjälp av sin mobiltelefon.

Metoden som visas i fig 5e är snarlik metoden enligt fig 5b, men kontrollen mot databasen 21 sker först efter en tidsfördröjning 48. Om mobilabonnemanget inte klarar kreditkontroll och ID-kontroll spärras mobiltelefonen i tjänsteleverantörens system. Exempel på användning av denna metod är betalning av kollektivtrafikavgifter, eller parkeringsavgifter.

Ytterligare varianter och kombinationer av dessa metoder kan förekomma inom ramen för uppfinningen. Antalet kodord som utbyts mellan mobiltelefonen och databasen kan variera beroende på den önskade säkerheten.

I det följande ges några exempel på situationer då en verifikationsmetod enligt uppfinningen är speciellt lämplig.

Restaurang

En gäst som ätit på en restaurang beställer av sitt kontokortsföretag eller liknande tjänsten att betala restaurangnotan med medel som finns på gästens eget konto eller på kontokortsföretagets konto (kreditkort). Kortfö-

retaget är således tjänsteleverantör, och gästen är beställare.

På känt vis hanteras kontokortet av restaurangpersonalen, för att verifiera kortets nummer, dess giltighet, att medel finns på kontot, att kortet inte är spärrat etc. Kortföretaget får på detta sätt kännedom om beställarens identitet, exempelvis genom det unika kortnumret. Enligt en vanligt förekommande teknik dras kortet i en kortterminal, som via modem kontaktar kortföretaget och kontrollerar transaktionen.

Kortföretaget har i ett register information om att beställaren är ansluten till systemet enligt uppfinningen, och identifierar mobilteleabonnemangets telefonnummer. Detta skickas till databasen, vilken därefter kontaktar mobiltelefonen via telenätet och mottar ett kodord (fig 5a).

Alternativt använder beställaren sin mobiltelefon för att i samband med beställningen uppge ett kodord (fig 5b). Kodordet kan överlämnas till restaurangpersonalen, som via kortterminalen kontaktar kortföretaget och överför koden, eller också överföras från mobiltelefonen till kortterminalen genom någon form av kommunikationsorgan, exempelvis en IR-port.

När kodordet verifierats av kortföretaget skickas ett klartecken 47 till restaurangen, varvid ett kvitto skrivs ut.

Internettransaktion

Förfarandet är snarlikt när en datoranvändare vill göra en transaktion på Internet eller liknande, exempelvis göra en girering från ett av sina bankkonton, eller handla med ett kontokort. Datoranvändaren är då beställare av en tjänst i form av en transaktion. Tjänsteleverantören kan vara ett kortföretag enligt ovan eller beställarens egen bank.

Beställarens identitet överförs i detta fall genom en inmatning av exempelvis ett personnummer och tillhörande lösenord eller ett kontokortsnummer eller liknande.

En sådan inmatning kan ske i en skärmbild på en WWW-sida, varefter sidans innehåll med en knapptryckning skickas till sidans innehavare.

Om ett förfarande enligt fig 5a används blir förloppet identiskt med det ovan beskrivna exemplet, och beställaren får inom någon minut ett SMS-meddelande till sin mobiltelefon, och kan bekräfta beställningen genom lämpliga knapptryckningar. Om ett förfarande enligt fig 5b utnyttjas, där beställaren läser av ett kodord från mobiltelefonens display, kan kodordet överföras på samma sätt som identiteten, antingen på samma WWW-sida eller vid en efterföljande sida, som dyker upp så snart identiteten godkänts.

Inloggning/inpassering

Ytterligare en tjänstekategori som lämpar sig för verifikation enligt uppfinningen är inloggning i ett datorsystem. Beställaren är då personen som vill åtkomma systemet, tjänsten är att släppa in personen i datorsystemet eller liknande, och tjänsteleverantören är det företag eller datorsystem som är ansvarigt för säkerheten.

Beställaren anger sin identitet vid en inloggning enligt känd teknik, och uppger därvid exempelvis ett användar-ID med lösenord. Därefter kan tjänsteleverantören kontakta databasen som begär ett kodord direkt från mobiltelefonen enligt fig 5a. Alternativt kan beställaren enligt fig 5b ges möjlighet att via tangentbordet ange en kod som avlästs ur mobiltelefonens display.

Vid fysisk inpassering till en lokal eller ett område blir situationen snarlik den vid inloggning. Exempelvis kan då beställarens identitet anges genom att dra ett passerskort eller slå en kod på ett portlås.

Exempel på detaljerad händelsekedja vid betalning med kontokort

Nedan görs, med hänvisning till fig 6, en mer detaljerad beskrivning av en tänkbar kedja av händelser för att en legitim beställare skall kunna utföra ett uppdrag med mycket hög säkerhet. Om uppdraget inte har så hög sä-

kerhetsklassning kan vissa moment uteslutas ur händelsekedjan. Det är lämpligen tjänsteleverantörens dator som avgör vilken säkerhetsklass som uppdraget skall ha och om dricks ska lämnas till försäljningsstället. Därmed styrs resten av händelsekedjan baserat på säkerhetsklass och om dricks ska lämnas eller ej.

a) Beställaren 41 lämnar ifrån sig ett kontokort 51.

b) Kontokortet dras i kortterminalen 52 och betalningsbeloppet (inklusive eventuella garderobsavgifter mm) matas in i terminalen. Terminalen 52 genererar ett meddelande om önskad betalning som bl.a. innehåller kortnummer, kortterminalens nummer och betalningsbeloppet.

c) Kortterminalen skickar det i (b) genererade meddelandet till kontokortföretagets dator (tjänsteleverantören 42).

d) Kontokortföretagets dator kreditprövar transaktionen och om denna prövning faller väl ut så genererar datorn ett meddelande om transaktionen (säljare och belopp mm), uppdragsnummer, uppdragets säkerhetsklass, om "dricks" förekommer samt kontokortinnehavarens mobiltelefonnummer.

e) Kontokortföretagets dator skickar det meddelande som genererats i (d) till databasen 21.

f) Databasen 21 plockar fram nästa oanvända kodord, kollar med aktuell mobiloperatör 54 om mobilen är på en tillåten plats och genererar ett meddelande med begäran om bekräftelse av uppdraget. I meddelandet ingår bl.a. säljare, belopp, uppdragsnummer, säkerhetsklass, om dricks förväntas och nästa oförbrukade kodord (576362).

g) Databasen 21 skickar det meddelande som genererats i (f) till beställarens mobil 10.

h) Mobilen kollar vilken säkerhetsklass som gäller och om dricks förekommer. Baserat på detta väljer mobilen vilken rutin som skall verkställas. Mobilen lägger upp förfrågan på displayen och ber om bekräftelse. Beställa-

ren trycker på bekräfta. Om det är en hög säkerhetsklass begär mobilen att beställaren trycker in PIN-koden eller ett motsvarande lösenord som bara beställaren har i sitt huvud. Om det är ett säljställe (exempelvis restaurant) som tillämpar dricks, kommer det en fråga på mobilens display om beloppet skall höjas och då kan beställaren mata in ett nytt högre belopp. Mobilen ber beställaren att åter bekräfta och om beställaren på nytt bekräftar så genereras antingen ett eller två meddelanden beroende på säkerhetsklass. Båda meddelandena innehåller bl.a. mobiltelefonnummer, uppdragsnummer, säljare, belopp, slutligt belopp (om dricks) det första oförbrukade kodordet (576362) och nästa oförbrukade kodord (805209) och om mobiltelefonen har inbyggd GPS-mottagare så bifogas även GPS-koordinaterna. Mobilen noterar de båda kodorden som förbrukade. Hela detta steg (h) hanteras av mjukvaran 18 i mobiltelefonen 10, vilken kan utvecklas av en fackman på området.

i) Mobilen 10 sänder det i (h) genererade meddelandet till databasen 21.

j) Mobilen 10 sänder det i (h) genererade meddelandet till kontokortföretagets dator 42.

k) Databasen 21 kontrollerar meddelandet från mobilen och om båda kodorden är korrekta genereras ett ID-bekräftelsemeddelande i vilket bl.a de båda kodorden ingår och de båda kodorden noteras som förbrukade.

l) Databasen 21 sänder det i (k) genererade ID-bekräftelsemeddelandet till kontokortföretagets dator 42.

m) Kontokortföretagets dator kontrollerar meddelandet från mobilen (j) och ID-bekräftelsemeddelandet från databasen (l) och gör lämpliga jämförelser. Om allt faller väl ut så genereras en skrivorder som innehåller lämpliga uppgifter exempelvis säljare, köpare, belopp, kontokortsnummer, uppdragsnummer, datum, klocka och verifikationsnummer.

n) Skrivorden överföres till kortterminalen 52.

o) Kortterminalen skriver ut transaktionskvittot 53.

p) Beställaren får tillbaka kontokortet 51 och skriver under transaktionskvittot 53 och tar kopian medan säljaren behåller originalet.

Följande är vad beställaren upplever av ovanstående händelsekedja.

- Beställaren lämnar sitt kontokort som vanligt.
- Beställaren får upp betalningen på sin mobiltelefondisplay inom någon minut och bekräftar uppdraget genom två knapptryckningar. Vid stora uppdrag (hög säkerhetsklass) får beställaren mellan den första och andra bekräftelsen, mata in PIN-koden eller annat liknande lösenord och eventuellt justerar upp beloppet, d.v.s. ger dricks.
- Beställaren får skriva under transaktionskvittot och ta kopian som vanligt.

Tillkommande moment: Beställaren bekräftar genom två knapptryckningar betalningen plus matar eventuellt in PIN-kod och höjer beloppet om dricks ska ges.

Moment som försvinner: Beställaren slipper att visa legitimation.

Följande är vad säljaren upplever av ovanstående händelsekedja.

- Säljaren tar kontokortet och drar detta genom kortterminalens läsare som vanligt.
- Säljaren matar in beloppet via kortterminalen som vanligt.
- Säljaren river av transaktionskvittot som vanligt.
- Säljaren tillser att beställaren skriver under transaktionskvittot och tar originalet som vanligt.

Tillkommande moment: Inga

Moment som försvinner: Säljare slipper begära legitimation, kontrollera legitimation och skriva legitimationsnummer.

<u>Tänkbara varianter på ställen där betalningen måste ske snabbt</u>

Man kan exempelvis vid betalning av mindre belopp i affär, kiosk, bensinstation mm tänka sig att bekräftelsen inte sker över mobilnätet, eftersom detta kan ta någon minut extra. Istället kan exempelvis mobiltelefonens infraröda dataöverföringsport 19 användas. I detta fall utrustas också kortterminalen med en motsvarande kommunikationsport (ej visad) och programvara, samt en display om inte kassaapparaten redan har en display riktad mot kundsidan. Kommunikationsporten sitter lämpligen i displayenheten eller nära denna.

För denna utförandeform drar säljaren beställarens kontokort och matar in beloppet eller får det direktöverfört från exempelvis den bensinpump som beställaren just använt d.v.s. som det fungerar idag. När detta är klart visas beloppet på ovan nämnda display, vilken också uppmanar beställaren att exempelvis "Bekräfta betalningen med din mobil". Beställaren riktar sin mobil mot displayen och mottar exempelvis bensinstationens namn och det aktuella beloppet. Genom två bekräftelsetryckningar på mobilen så överföres det första oanvända kodordet till kortterminalen och displayen kan exempelvis visa "Lösenord mottagits". Därefter fungerar allt som idag.

Man kan säga att mobilen ersätter den kontrollknappsats som är vanlig på många bensinstationer i åtminstone Sverige. Någon som står bredvid kan emellertid se vilken kod som slås in även om det finns ett skydd som skall göra det svårare att se. Om den som just slog in sin kontrollkod skulle glömma sitt kort på disken föreligger en frestelse för en oärlig person. En sådan person skulle kunna lägga handen över den förra kundens kontokort och låta det glida ner i fickan. Den oärlige personen skulle sedan kunna tanka upp exempelvis familjens bilar innan kortets riktiga ägare någon vecka senare skall tanka sin bil på nytt och märker att kontokortet är borta.

Uppfinningen innebär ju att ett kodord aldrig används mer än en gång och för övrigt är det normalt ingen, varken beställaren eller annan, som ser några kodord över huvud taget.

Avslutning

Det inses att en mängd varianter av de ovan beskrivna utföringsformerna är möjliga inom ramen för de bifogade patentkraven. Exempelvis kan ett stort antal alternativa verifikationsförfarande genomföras med ett system enligt uppfinningen. På samma sätt kan annorlunda utrustning än den här beskrivna användas för att verkställa metoden enligt uppfinningen.

PATENTKRAV

1. Metod att verifiera uppdrag från en beställare (41) till en tjänsteleverantör (42), innefattande stegen

att bilda ett flertal uppsättningar (1) slumpmässigt framtagna kodord (2),

att lagra en av nämnda flertal kodordsuppsättningar (1) i en till ett mobilteleabonnemang associerad minneskrets (15) i en mobiltelefon (10),

att lagra en identisk kodordsuppsättning (1) i en databas (21) tillsammans med en association till nämnda mobilteleabonnemang, och

att vid beställningstillfället identifiera nämnda mobilteleabonnemang, utvinna åtminstone ett kodord (46) ur minneskretsen och kontrollera att kodordet förekommer i den kodordsuppsättning (1) i databasen som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

2. Metod enligt krav 1, varvid kodordet utvinns från minneskretsen (15) enligt en förutbestämd ordning, vilken ordning är känd av databasen.

3. Metod enligt krav 2, vidare innefattande steget att i åtminstone den ena av minneskretsen (15) och databasen (21) markera när ett kodord (46) har använts, varigenom säkerställs att nämnda förutbestämda ordning följs.

4. Metod enligt något av föregående krav, varvid steget att identifiera mobilteleabonnemanget innefattar stegen

att bestämma beställarens identitet, och

att utifrån beställarens identitet identifiera mobilteleabonnemanget.

5. Metod enligt något av föregående krav, varvid en begäran (45) att uppge ett kodord skickas till beställaren.

6. Metod enligt krav 5, varvid begäran (45) skickas till mobiltelefonen (10) via telenätet.

7. Metod enligt krav 5 eller 6, varvid kodordet överförs från mobiltelefonen (10) till databasen (21) via telenätet.

8. Metod enligt krav 1 - 3, varvid

beställarens identitet (43) och det ur minneskretsen utvunna kodordet (46) överförs till tjänsteleverantören (42),

mobilteleabonnemanget som är associerat till beställaren identifieras av tjänsteleverantören, och

kodordet (46) och mobilteleabonnemangets identitet (23) överförs till databasen av tjänsteleverantören.

9. Metod enligt något av föregående krav, varvid ett andra kodord (46'') utvinns från minneskretsen (15) och överförs till databasen (21), för att ytterligare verifiera uppdraget.

10. Metod enligt krav 9, varvid kodorden i uppsättningen är associerade till varandra i grupper (3), och nämnda första (46') och andra (46'') kodord ingår i samma grupp kodord.

11. Metod enligt krav 9 - 10, varvid nämnda första kodord (46') överförs från beställaren (41) till databasen (21), databasen skickar en begäran (45) till beställaren att uppge nämnda andra kodord (46''), varvid nämnda andra kodord överförs från beställaren till databasen (21).

12. Metod enligt något av föregående krav, vidare innefattande stegen

att till mobilteleabonnemanget associera och i databasen (21) lagra åtminstone en positionsangivelse (24),

att vid varje beställningstillfälle bestämma var minneskretsen (15) är lokaliserad, och kontrollera den sålunda erhållna positionsangivelsen med nämnda, i databasen lagrade positionsangivelse (24).

13. Metod att verifiera ett uppdrag från en beställare till en tjänsteleverantör, varvid en uppsättning (1) slumpmässigt framtagna kodord (2) har lagrats i en till ett mobilteleabonnemang associerad minneskrets (15) i en mobiltelefon (10) samt i en databas (21) tillsammans med en association (23) till nämnda mobilteleabonnemang, innefattande stegen

att bestämma beställarens identitet (43),

utifrån beställarens identitet identifiera mobilteleabonnemanget,

att utvinna ett kodord (46) ur minneskretsen, och

att kontrollera att nämnda kodord förekommer i den kodordsuppsättning (22) i databasen (21) som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

14. System för verifiering av ett uppdrag från en beställare (41) till en tjänsteleverantör (42), innefattande

en mobiltelefon (10) med en till ett mobilteleabonnemang associerad minneskrets (15),

organ för att låta beställaren till tjänsteleverantören uppge sin identitet (43),

kännetecknat av att systemet vidare innefattar

en databas (21),

en uppsättning (1) slumpmässigt framtagna kodord (2), vilken uppsättning för det första är lagrad i minneskretsen (15), och för det andra är lagrad i databasen

(21) och där är förknippad med mobilteleabonnemanget,

organ för att utifrån beställarens identitet (43) identifiera mobilteleabonnemanget,

organ för att låta beställaren (41) utvinna ett kodord ur minneskretsen (15), och överföra nämnda kodord till databasen (21), och

kontrollorgan (25, 26) för kontrollera att nämnda kodord förekommer i den kodordsuppsättning (22) i databasen som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

15. System enligt krav 14, varvid kontrollorganet innefattar ett kommunikationsorgan (25) för att kommunicera mellan databasen (21) och mobiltelefonen (10).

SAMMANDRAG

Uppfinningen avser en metod och ett system för att verifiera ett uppdrag från en beställare (41) till en tjänsteleverantör (42), varvid en uppsättning slumpmässigt framtagna kodord har lagrats i en till ett mobilteleabonnemang associerad minneskrets i en mobiltelefon (10) samt i en databas (21) tillsammans med en association till nämnda mobilteleabonnemang. Metoden innefattar stegen att bestämma beställarens identitet (43), att utifrån beställarens identitet identifiera mobilteleabonnemanget, att utvinna ett kodord (46) ur minneskretsen, och att kontrollera att nämnda kodord förekommer i den kodordsuppsättning i databasen (21) som är associerad till nämnda mobilteleabonnemang, för att därigenom verifiera uppdraget.

Publ. bild = fig 5a